EXPLAINING POLICY DIFFERENCES AS A FUNCTION OF DIVERSE GOVERNANCE INSTITUTIONS

A Dissertation
Presented to
The Academic Faculty

By

Jim Flowers

In Partial Fulfillment
Of the Requirements for the Degree
Doctor of Philosophy in Public Policy

Georgia Institute of Technology

And

Georgia State University

May 2016

EXPLAINING POLICY DIFFERENCES AS A FUNCTION OF DIVERSE GOVERNANCE INSTITUTIONS

Approved by:

Dr. John C. Thomas
Andrew Young School of Policy Studies
Georgia State University

Dr. Gordon Kingsley
School of Public Policy
Georgia Institute of Technology

Dr. Christine Roch
Andrew Young School of Policy Studies
Georgia State University

Dr. Seymour E. Goodman
School of International Affairs
Georgia Institute of Technology

Dr. Paul Baker
School of Public Policy
Georgia Institute of Technology

Date Approved: 29 February 2016

Acknowledgements

Just like the turtle on the fencepost, this work would not have happened without the support and assistance of others. When Dr. Kingsley assigned a paper by Ostrom and Gardner (1995) explaining the concept of the Institutional Grammar Tool, he asked the class to "tell me what you think of this notion and whether it has value?" I initially dismissed the paper as not relevant to my areas of interest. Little did I know how deep into the study of institutional analysis those concepts would take me.

I appreciate the patience and support of my committee members over the life of this project. I thank my chair, Dr. John Thomas, for being both understanding and insistent in a way that never discouraged but helped me to stay on task. I deeply appreciated Dr. Baker's willingness to look at very early drafts of my proposal, and for his insistence that I stay away from "squishy" concepts and measures. I thank Dr. Roche for patiently sitting through a number of trial presentations over the years as I struggled to find the most effective means of explaining what I did and why this project matters. I thank Dr. Goodman for his body of work on the topic of information and cyber security policy that serves as a foundation for much of the context of the policies that served as the subject matter for this study.

This project, like many, took on a life of its own. My friends and colleagues did their part to encourage and pester me to finish. Tom Lewis, who has been a colleague for some time, once said that asking me when I would finish reminded him of the Bullwinkle cartoon where Bullwinkle attempts to pull a rabbit out of his hat. No matter

how hard Bullwinkle tried, that rabbit never appeared. Similarly, this dissertation failed to appear as quickly as I, and my family and friends and committee members, would have liked. I thank all of them for their continuous encouragement, and their consistent admonition to “finish it!”

Family played a big role in the success of this project. I thank my father-in-law for allowing me to turn his kitchen into my place to write. I owe my youngest boys thanks for understanding that I could not always play on Saturdays and Sundays. There is no measure of what I owe my wife, Kristy. I will be forever grateful to her for her love and support.

Table of Contents

List of Tables

List of Figures

List of Abbreviations

ACUPA	Association of College and University Policy Administrators
AGILE	Not an acronym – references the philosophy for software development, as described in *The Manifesto for Agile Software Development,* where "requirements and solutions evolve through collaboration between self-organizing, cross-functional teams".
BOR	Board of Regents
CIO	Chief Information Officer – normally the top IT manager at the university
CISO	Chief Information Security Officer
DHS	Department of Homeland Security
GS	Georgia Southern
GSU	Georgia State University
GT	Georgia Tech
ISO	International Standards Organization
NIST	National Institute of Standards and Technology
UGA	University of Georgia
USG	University System of Georgia

Summary

This study asks the question: "How does the structure of cybersecurity policy relate to differences in structure of policy governance of universities and colleges?" The study has three objectives. First, the study seeks to add to the body of knowledge concerning the relationship between the structure of cybersecurity policy processes and the security policies developed by those processes. Second, the study seeks to demonstrate the usefulness of the Institutional Grammar Tool, Rules Configurations, and other methods employed to analyze institutional configurations. Third, the study seeks to provide pragmatic suggestions for cybersecurity practitioners to systematically identify deficiencies in policy structure that contribute to less than optimum outcomes.

Research on this question is necessary as no integrative framework exists for describing or predicting how organizations adopt and implement cyber security policy. The study proposes such a framework by integrating an ideal model for cyber security governance with the principles of the Institutional Analysis and Design framework (IAD). Four research universities of the University System of Georgia are subjected to a cross-case comparison of information security policies. Interviews and policy documents provide a database of institutional statements that are analyzed using IAD methods and tools.

Prior research suggests that elements of policy structure, such as how the policy fits the organization's objectives and culture, are linked to policy effectiveness. Research also suggests that how those elements of policy structure reflect external threats and

organizational factors are determined by how the cybersecurity policy development is integrated into the governance of university wide policy.

In addition to demonstrating the utility of an integrated approach to studying the problem of creating effective policy, findings demonstrate how a well-integrated cybersecurity governance structure provides better fit, constructs policies of appropriate scope, and is more likely to include the components of governance necessary for policy effectiveness. Findings also suggest that policy form, the readability of policy, may be improved if the documents are analyzed using the institutional grammar tools suggested by the IAD and if collaboration with users and managers to construct policy is encouraged. The capability of the methods employed by the study to identify deficiencies in cyber security governance structure that are manifested in less effective policy outcomes may aid policy makers as they strive to develop policy solutions to an ever changing security threat.

Chapter 1 - Introduction

Researchers surveyed the world's top 100 universities in a quest to examine the structure and content of information security policies implemented (Neil Francis Doherty, Anastasakis, and Fulford 2009). The authors supposed that universities would be appropriately concerned with policies to protect the data, computers, and networks that support the administrative, education, and research missions of these organizations. However, the article found a "wide diversity of policies and standards" indicative of a non-uniform approach to security management. The issues covered by these policies were very narrow and reflected a "highly techno-centric view of information security management" (Neil Francis Doherty, Anastasakis, and Fulford 2009, 449). The study concluded that universities have not "tailored their policies to reflect their status as knowledge-intensive organizations" (Neil Francis Doherty, Anastasakis, and Fulford 2009, 456).

There is a significant gap in the literature with "respect to approaches to the formulation of information security policy" (Baskerville and Siponen 2002 as found in Doherty, et al. 2009). Knowledge about the challenges and constraints of policy processes that assess, create, and monitor security policy is minimal (Werlinger, Hawkey, and Beznosov 2009, 7). Policy advisors believe that understanding how organizations structure cybersecurity policies in response to varying threats and external mandates is worthy of additional research (Portnoy and Goodman 2009). The literature suggests that an understanding of the relationship between the structure of

policy process and policy content may improve the design of cyber security policy for organizations in the higher education sector (Neil F. Doherty and Fulford 2006; Neil F. Doherty and Fulford 2006; Werlinger, Hawkey, and Beznosov 2009; Knapp and Ferrante 2014).

This study addresses the research question: "How does the structure of cybersecurity policy relate to differences in structure of policy governance of universities and colleges?" Policy governance is conceptualized as a collection of processes that develop, review, approve, and implement information security policy. The governance structure is conceptualized by the actors and the rules assigned to each process designed to create, retire, and modify policy in alignment with organizational goals. Policy structure may be defined as the relationships between the objectives of policy and the policy elements available to achieve those objectives. Those elements include components of policy, such as guidelines, standards and procedures, that are written to delineate responsibilities and actions needed to affect outcomes. Other elements include the scope of issues addressed by the policy, the form of language used to communicate policy, and the fit of that policy relative to the organizational structure and culture. Taken together, these elements provide measures of structure that determine the likelihood of policy effectiveness.

I examine cyber security policy developed and implemented by the University System of Georgia (USG) and its 35 member institutions in a time period from 1999-2014 is examined. The USG colleges and universities are governed by a Board of Regents and that Board sets policy for the units to implement. Despite the collaboration

of the college and university CIO's within the USG to create system-wide policy the structure, content, and issues covered at each campus varied widely. Given each college and university operates under the same board policies then logically you may ask whether the difference in information security policy may be related to differences in how policy is made. Further, how might differences in the availability of the resources, the missions, and the governance of these organizations contribute to the differences in policies? What role do these factors play in the various styles of information security policy found at each campus?

In the next section, I will highlight some of the challenges for design and implementation of security policy that are unique to the higher education sector. Next, I provide a summary of relevant USG policies to provide context. A brief introduction to the theoretical framework and theories applied to this study follows. I close the chapter with an outline of the work to follow.

1.1 Cyber Security Issues and the Higher Education Sector

> *It would be convenient if we could solve security problems by installing a piece of technology, but the truth is that security is as much an issue of people and process as it is technology.*[1]

Prior to 2000, the research literature for cybersecurity focused on technological challenges (R. Anderson and Moore 2009). One literature review calculated that 94 percent of "public research in computer security had concentrated on technological

[1] Oblinger, Diana G., and Brian L. Hawkins. 2006. "The Myth about IT Security." *EDUCAUSE Review Magazine*, January 1.

advances" (Beznosov and Beznosova 2007). Most organizational security practices also focused on technical solutions (Gurpreet Dhillon and Backhouse 2001; M. Siponen, Pahnila, and Mahmood 2010; Mikko Siponen and Iivari 2006), ignoring the organizational and human aspects of the problem. Policymakers suggest that a focus on technical solutions while ignoring nontechnical factors may contribute to the lack of adoption of the technical solutions (Goodman and Lin 2007, 131).

A number of reviews and studies call for a holistic model of security research that recognizes the human, organizational, and technological dimensions to the phenomena that must be understood (Dhillon and Backhouse 2001; Albrechtsen 2007; May and Dhillon 2010; Kolkowska and Dhillon 2013; Zuccato 2007). The human dimension focuses on the phenomena of individual behavior as a major factor in the outcome of security policies and practices (G. Dhillon and Backhouse 1996). Organizational dimension include concepts like culture, top management support, and environmental certainty (Knapp et al. 2006). The correlation of the direction and size of these factors upon security outcomes has been documented by a number of studies (Knapp et al. 2009; Baskerville 2006; Berardo 2009; S. E. Chang and Lin 2007; Werlinger, Hawkey, and Beznosov 2009; Hsu, Lee, and Straub 2012).

The suggestion of a holistic approach from academics is echoed in a survey of members of the higher education security community that identified the top three issues of concern for 2016:

1. Ensuring that members of the institutional community (students, faculty, and staff) receive information security education and training

2. Developing an effective information security strategy that responds to institutional organization and culture and that elevates information security concerns to institutional leadership
3. Developing security policies for mobile, cloud, and digital resources (including issues of data handling/protection, access control, and end-user awareness[2]

The importance of concepts such as top management support; security awareness and training; and effective policy development were recognized by the higher education community in the early 1990's as essential to effective security (Elliot et al. 1991). If you substitute the term "personal computer" for "mobile, cloud, and digital resources" in item 3, then the top 3 issues of 2016 and 1991 have not changed. And, despite 25 years of effort and experience, the attacks on higher education computing resources continue to increase in terms of frequency and cost[3].

A university or college is targeted for attack for one of two main reasons: first, the computing resources possessed by universities have tremendous aggregate capabilities; second, the philosophy protecting access to information and information resources makes these resources a vulnerable target (Katz 2005). It is unreasonable to propose that higher education diminish the inventory of computing resources in order to avoid cyber attacks. Open and "free" access to knowledge, information, and the resources to access both, are essential values of higher education organizations. A university must protect technology and data from unwarranted and malicious access

[2] Grama, Joanna Lyn, and Valerie M. Vogel. "The Top 3 Strategic Information Security Issues." *EDUCAUSE Review Magazine*, January/February 2016.
[3] Smith, D. Frank. "EDUCAUSE 2014: Cyberattacks Are a Growing Problem for Higher Education." Magazine. *EdTech*, October 6, 2014. http://www.edtechmagazine.com/higher/article/2014/10/educause-2014-cyberattacks-are-growing-problem-higher-education.

while supporting the mission of the organization, and securing the values and trust of its individual members. The task is not a trivial one. The next three sections highlight the challenges for each of the three dimensions within the cybersecurity challenge.

1.1.1 Organizational Dimension

Organizational structure, culture, and resources vary widely within higher education (Nicholson-Crotty and Meier 2003). Millett observed that "University departments, centers of research, colleges and schools present a distribution of authority that contains hierarchical as well as horizontal lines of authority" (1962, 61). He describes "communities of power" organized in four constituent groups; faculty, students, alumni and administration, that confound attempts to centrally organize or administrate higher education (p. 62). A school, or college, may maintain functions to manage academic, business, student, and information system needs that are duplicated in other schools and divisions of the university. Such is the organizational structure that Cohen and March (1972) described as a form of organized anarchy with a policy process best euphemized as akin to producing good eats from a "garbage can". Weick (1976) described the structure of higher education as resembling one of many "loosely coupled systems."

The culture and the mission of many universities expects and emphasizes the open exchange of knowledge and therefore is resistant to efforts to "lock down" information technology (Hess and Ostrom 2004). Efforts to manage the tension between open data and secure systems are often frustrated by the lack of resources

necessary to fund them[4]. Competitiveness and the desire to reap commercial benefits from original research drive the desire of universities to maintain layers of protection of developed, and developing, intellectual properties. A security regime may need to accommodate different levels and types of data access and data security from one laboratory to the next.

Obviously, educating students is the primary task of higher education. Those students may have a myriad of experiences and needs. A campus today may have a student population of average age 29 that reflects enrollment of ages 14 to 80. Students may be housed in campus or proximate housing, or may commute. Students may acquire a degree using distance learning technologies, or a mix of on-campus, at a distance, and hybrid course delivery strategies. Providing access to the electronic delivery of courses, books, articles, and lectures requires an open and robust technology infrastructure. Security procedures cannot inhibit access for fear of increasing the costs of educating students, and, perhaps, decreasing the retention of students for which significant resources were expended to recruit. A campus that provides healthcare and residential support for students also agrees to protect the privacy of student health and lifestyle choices. Many of these services are provided by private, third party vendors,

[4] "…higher education institutions are strapped for resources to manage the balance between openness and security against malware and sensitive data exfiltration, according to nearly 300 higher education IT professionals who took a SANS survey conducted in February and March 2014. In the survey participants confirmed the historical difficulties of making their environments secure while also providing the openness institutions need for their students, staff, parents and benefactors. As one write-in response stated, "University culture often conflicts heavily with the need for robust security: Adjusting the culture would allow more emphasis on security controls." Marchany, Randy. *Higher Education: Open and Secure?*. A SANS Analyst Survey. SANS ANALYST PROGRAM, June 2014. https://www.sans.org/reading-room/whitepapers/analyst/higher-education-open-secure-35240.

who use technology that is not under the direct supervision of campus security policies. These services are also attacked and present another layer of challenges to campus security[5].

Autonomy is a significant feature within the campus governance structure (Blau 1994). Autonomy is found at all levels of the organization from the individual faculty member to the systems and associations that govern public institutions of higher education (Christensen 2010). The influence of autonomy contributes to the nature of the organizational structure and the structure is designed to protect the value held by the community. Autonomy may frustrate efforts to motivate change and innovation, whether driven by external mandates or internal evolution, even as many pieces of college organization attempt to collaborate (Bartell 2003).

The level of awareness of these issues within top management is a fundamental predictor of effective security policy (Rezgui and Marks 2008). The degree of top management support is often reflected in the alignment of policy to organizational mission; the allocation of resources to implement, maintain, and monitor the policy; and in the culture of the staff, employees and customers who take their cues from upper management. If top management is sufficiently aware, then the alignment of university objectives and security policy is more likely to occur and the desired outcome is more likely as well (Sabherwal and Chan 2001). Unfortunately, top management within

[5] Oblinger, Diana G., and Brian L. Hawkins. "The Myth about IT Security." *EDUCAUSE Review Magazine*, January 1, 2006.

universities are not likely to acknowledge the problem as one that needs more than a technical solution (Neil Francis Doherty, Anastasakis, and Fulford 2009).

External pressures from state and federal governments to protect student data, employee data, intellectual property, and healthcare data may conflict with that culture and competes for available resources. Economic, legal, and national security requirements may include provisions of secrecy or security that frustrate openness and transparency. Indeed, some universities are targets of foreign governments due to the research done on behalf of the military and intelligence agencies[6]. Public universities are often subject to requirements that records be open to public inspection. And, expectations from external groups such as the payment card industry (PCI), recording and movie industry, research and development partners, and privacy advocacy groups, to name a few, add to the challenges of designing effective policy.

1.1.2 Human Dimension

The second dimension of cybersecurity is the human dimension. Once policy is developed and approved, users (the students, staff, and faculty) must be made aware, and perhaps trained, as to implementation of the policy, and the particular objectives or outcomes that the policy is designed to produce (Goodman and Lin 2007). "Unintentional human error" and insider threats constituted more than a third of data breaches that occurred within higher education organizations in the time period of

[6] http://www.bloomberg.com/news/print/2012-04-30/military-secrets-leak-from-u-s-universities-with-rules-flouted.html.

2005-2013[7]. Training and awareness is an important tool in the fight to decrease the frequency of breaches.

The diversity of stakeholders within higher education organizations is another challenge unique to the sector. In addition to the four constituent groups identified by Millett (1962), organizations in this sector have a number of external groups that include federal, state, and local governments that create requirements to protect the privacy of data related to concerns that involve healthcare, financial, and intellectual property data. In addition to external stakeholders, internal stakeholders provide a complex environment rich with opportunities for concepts to interact. For example, individual variation of perception of risk and the distribution of security information to individuals via a distributed management system – may affect the scope of policy as risk and perceived costs affect the analysis of cost and benefits (Werlinger, Hawkey, and Beznosov 2009, 13).

An organizational culture that is "security aware" improves the likelihood of employee compliance to formal security rules (Goo, Yim, and Kim 2013; Goo, Yim, and Kim 2013; Hawkey et al. 2008). Large organizations are more likely to invest in the adoption of security standards given their increased reliance on formalization (i.e. hierarchy), increased awareness and value of information assets, and greater access to necessary resources such as trained IT staff and cash (S. E. Chang and Ho 2006). The positive support of organizational executives is a necessary requirement for creation of

[7] Data found in **Data Breach Readiness and Follow-up: Being Prepared for the Inevitable** at https://www.privacyrights.org/content/data-breach-readiness-and-follow-being-prepared-inevitable. Last accessed 25 May 2015.

effective policy and policy management (Knapp et al. 2009, 2) and is a predictor of organizational capability (Hsu, Lee, and Straub 2012). The role of environmental factors that affect an organization, such as rapidly changing technology, increase in threats from nation states and cyber criminals, and multiple and changing laws, regulations, and legal requirements, is an important contributing element determine an organization's security structure and outcomes (S. E. Chang and Ho 2006; Baskerville 2006; Knapp and Ferrante 2014).

Both current and former employees are found to be a primary cause of security incidents (da Veiga and Martins 2015). Research on employee compliance to organizational security rules has identified education, training, and awareness programs as important to affecting desired outcomes (Bulgurcu, Cavusoglu, and Benbasat 2010). If employee training and awareness programs are not supported adequately, then the effects of investments in cybersecurity technologies is not fully appreciated (K. Chang and Wang 2011). The inclusion of employees in the development, implementation, education, and maintenance of policies contributes to collaboration between security practitioners and the individuals whose behavior is to be modified by policy (Werlinger, Hawkey, and Beznosov 2009).

However, resources are required to produce the tools to provide training. Resources are required to create means of improving awareness of the policies and the respective objectives. And, resources are required to ensure that staff, faculty, and students take the time required to engage in the training and awareness activities. But, these requests must compete with requests to fund programs to improve the

acquisition and retention of faculty and students; to improve campus safety; to improve graduation rates; and so forth. Top management support from outside the information technology department is essential to the success of such requests.

1.1.3 Technology Dimension

The third leg dimension focuses on technology. Information technology changes at a pace that challenges the resilience of policies and procedures employed to secure data and other cyber assets from harm, both intentional and unintentional (Hess and Ostrom 2004). Recent investments in technology become outdated, or are rendered useless, due to technology changes. Advances in security may be slowed by regulator processes that do not inhibit illegitimate uses to proceed. As the bad guys get smarter, an organization must make its employees, both technical and non-technical, aware of the challenges and solutions to defeating these efforts. Acquiring new technology, upgrading old technology, educating and training managers, staff, and customers require resources that are scarce in most organizations, even more so in most higher education organizations.

A university network is constructed to encourage access to information and the free-flow of communications (Drevin, Kruger, and Steyn 2007). The requirement of open environments for research and knowledge exchange is an important tenet of academic freedom, and represents a serious challenge to the implementation of security policies (Hawkey et al. 2008). The AAUP has written extensively on the importance of academic freedom and more recently on the need to balance access to information with the need for security (Reichman et al. 2014). So it is not surprising that

the president of a USG institution, when pressed to shut down those networks involved in the Pentagon attack, cited academic freedom in defense of not enforcing security policy prior to the attacks and not immediately disconnecting the attacking computers.

The N-device problem, a name for the multiple devices (e.g. smartphones, tablets, and watches) employed by individuals, present additional challenges to security. Several years ago, a device would be a desktop or laptop computer. Today, that device category includes a number of wearable, portable, and stationery devices including laptops, tablets, phones, watches, and phablets. Individuals will use these devices simultaneously, thus creating an access problem that challenges the traditional design of most campus information technology architecture. Networks deployed less than 10 years ago cannot support a class of 35 students when each student has 3 or more devices requesting access to a network. A device that could accommodate 40 laptop connections is now expected to support more than 130 connections. Each of those devices presents a potential weak point in campus security. A lost, or compromised, device can allow access to data that is not permitted. Similarly, the use of third party "cloud" storage services by faculty, staff, and students presents another point of potential compromise when data is stored "off campus" and those services are attached. Such a compromise may result in campus non-compliance with student expectations of confidentiality, federal legal protections of confidentiality, and commercial contractual obligations of protection of data.

Higher Education has formidable challenges to overcome in the design of effective cyber security policy. Observations from researchers and practitioners concur

that little has changed in terms of the top concerns of policy makers assigned the task of securing the cyber assets of higher education. The question then is why is implementation of effective security policies seemingly difficult within the sector? The next section describes the theoretical framework identified to answer the question.

1.2 Overview of Theoretical Framework

The theoretical frame guiding this study is based upon these findings gathered from the information security research discipline (Figure 1-1). First, according to Höne and Eloff , effective cyber security is a product of effective cyber security policy (2002b). Second, effective security management can influence the effectiveness of security policy and thus precedes effective outcomes (Hicklin and Godwin 2009). Higgins and others find that effective cyber security management is preceded by effective policy (Higgins 1999; Fulford and Doherty 2003; Straub and Welke 1998). Effective security policy and effective security management are products, or outcomes, of an organization's cybersecurity policy process (Knapp et al. 2009).

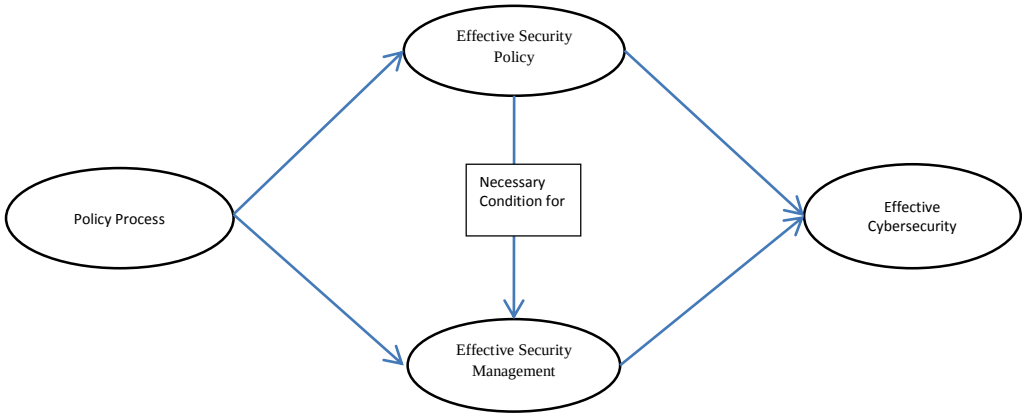

Figure 1-1 Theoretical Frame

The framework suggests that deficiencies in the structure and content of security policy may be explained by understanding the organization's policy process. However, the literature from the field of information security is weak in regards to understanding security policy processes (Whitman 2008). One review suggests the sum total of research on the effects of process on policy is "that the nature and scope of the information policy process impacts the nature and scope of the information policy and possibly the policy outcome" (Jones and Chudoba 2012).

Baskerville and Siponen (2002) reviewed the information security literature and reported that two levels of policy are commonly identified. High-level policy states the organizational goals and objectives while documenting management and employee responsibilities to protect organizational information resources (p. 339). The authors cite an example:

> *Departments should ensure that adequate information security management policies are implemented to protect their information asset.*

Lower-level policy focuses on individual methods or steps of actions to guide individual level decisions. Again, the authors cite an example:

> *You (user) will be required to change your password at least every 90 days.*

The authors noted that the literature did not contribute much to the topic of how policy is created, implemented, enforced, and monitored for effectiveness. Changing external conditions, including changing technology, places demands on organizations to adapt information security policies that are capable of adjusting quickly. Organizations that are constantly changing identify as "emergent organizations" (Truex, Baskerville,

and Klein 1999). Emergent organizations require adaptive information systems and policies that support and protect such systems. That requirement necessitates a policy process capable of determining when and how policies, standards, and guidelines should adapt to changes whether internal or external to the organization. The authors suggest that research should focus on a third-level of policy, a meta-policy or a "policy about policies", designed to establish "how information security policies are created, implemented, and enforced" (Baskerville and Siponen 2002).

The Knapp model[8] is a holistic framework focused on questions as to how a security policy process and the external and internal influences contribute to effective (i.e. successful) security policies (p. 502). The model (see Figure 1-2) identifies a policy process (e.g. a governance structure) that defines how policy is created, implemented, enforced, and maintained. The model identifies intervening effects of the organizational environment (e.g. context); internal influences which include senior management support, organizational culture, and internal threats; and external influences, which include policy mandates, technology changes, and external threats. The cycle of policy processes shown is similar to the policy stages heuristic that has been so influential in public policy research (Sabatier 2007a). The inclusion of feedback loops is a modification encouraged by advocates of the stages heuristic (Eger and Marlowe 2006) as well as by researchers in the domain of quality management and cybernetics (Wiener 1948; Deutsch 1963; Ali, Soomro, and Brohi 2013).

[8] The policy process model will be referenced from this point on as the Knapp model for brevity.

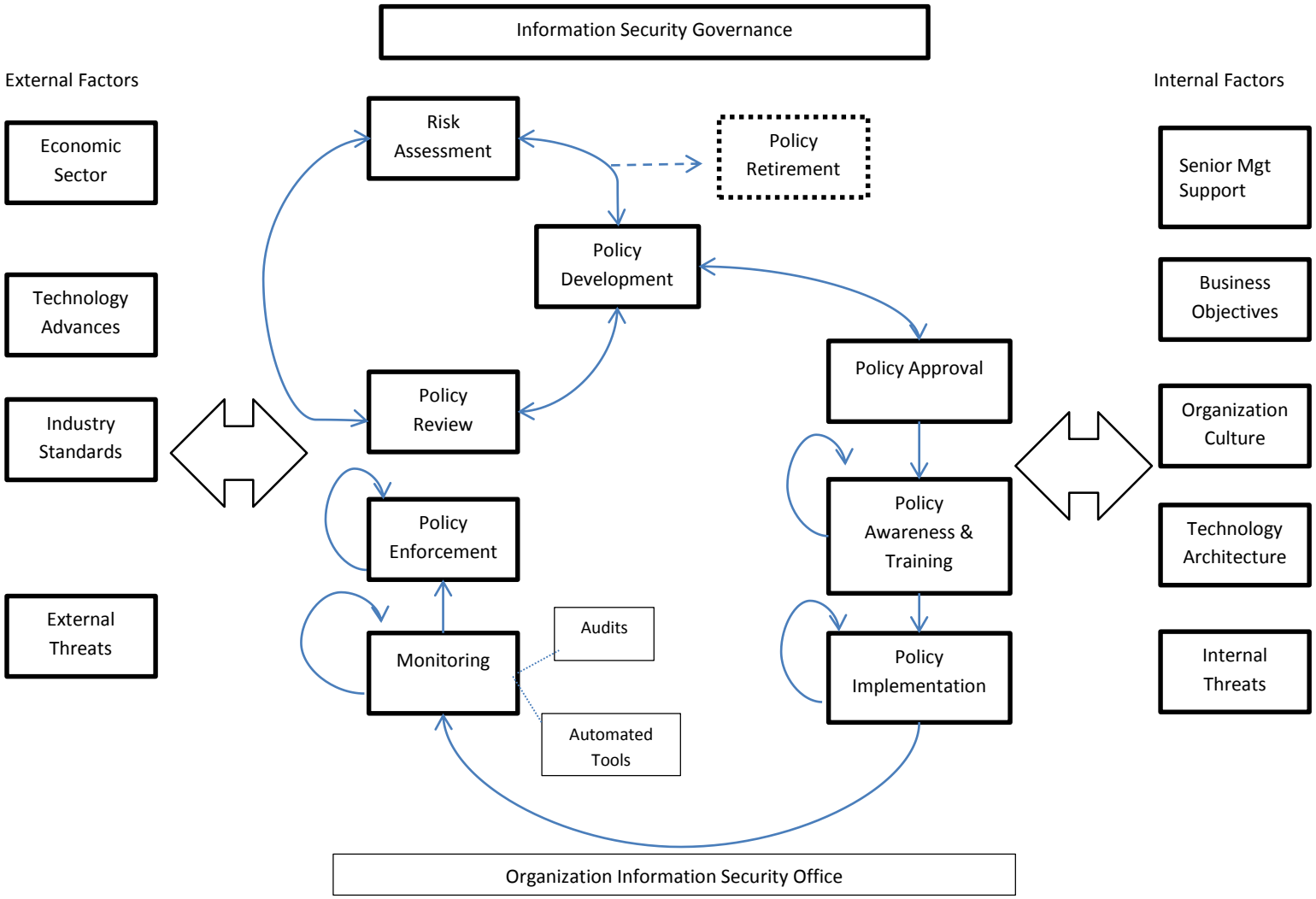

Figure 1-2 Policy Process Model

Source: Knapp, et al 2009

The Knapp model suggests there is a structure to meta-policy that can be identified and measured with regards to the steps or tasks required, the institutional constraints, and the actors involved. The steps or activities that structure the policy process (e.g. development, review, awareness, etc.) describe the elements of a meta-policy. Measuring that structure requires an instrument that can systematically identify the institutions, actors, and other influences of the policy process.

Aligica promotes the utility of the IAD framework as a tool to map structure (Aligica 2006). The IAD framework has provided considerable conceptual and empirical contributions with regards to institutions and the role that institutions play in the policy process (Kiser and E Ostrom 2000; E Ostrom 1986, E Ostrom 1990, E Ostrom 2005; E Ostrom and Hess 2007). Ostrom suggests that identifying “an outcome consistent with a pattern [of policy structure] may be the best verification we can achieve in settings of substantial complexity” (2005, 11). The tools and methods employed to use them are a means that "produces generalizable knowledge on the interaction of policy designs and policy processes, and resulting policy design divergence" (Carter et al. 2015). Recent works have focused on tools developed within the framework to classify institutions as specific rule types and to identify structural elements of institutions in a valid and reliable way (Basurto et al. 2010a; Carter et al. 2013; E. Ostrom and Basurto 2011; S. Siddiki, Basurto, and Weible 2010). Specific to this study, these new approaches promise to reliably document and assess policy change (Weible and Carter 2015).

1.3 USG IT Policy

The cases selected for this study are public universities that are members of the University System of Georgia and are governed by a Board of Regents[9]. In March of 2008, the Governor of Georgia signed an executive order (appendix A) requiring all state agencies to report on the status of their information security programs. Per this order, all state agencies are required to provide specific reports as determined by the state auditor and state CIO. Further, the Governor's order advocated the implementation of the standards and compliance framework mandated by the Federal Information Security Management Act (FISMA) upon federal government agencies. The Regents, responding to the Governor's executive order, initiated significant changes to the University System's cyber security policy and the respective cyber security policies of the institutions of the USG.

The 35 units of the USG[10] include four research universities (Carnegie Classification R-1), 2 regional universities, 13 state universities, 8 state colleges and 6 two year colleges. The schools within the USG present differences, some subtle and others not so subtle, in terms of organizational structure, resources, mission, and geographic location. USG policy statements direct policy makers at each unit as to the construction of policy, the goals of policy, and the tactical implementation of policy.

[9] Constitution of the State of Georgia, Article VIII, Section IV, Paragraph (b).
[10] Since 2012, the USG has consolidate 12 institutions – so the total is 29 as of this writing.

For example, the strategic plan of the University System Office of Information Security set the following expectations for campus information security governance[11]:

> Effective security governance is managed as an organizational-wide issue that is planned, managed and measured in all areas throughout the organization. In IT Governance, leaders are accountable for and are committed to providing adequate resources to information security. A core set of principles to guide the framework for governance should include:
>
> - Conduct an annual information security evaluation, review the evaluation results with staff, and report on performance.
> - Conduct periodic risk assessments of information assets as part of a risk management program.
> - Implement policies and procedures based on risk assessments to secure information assets.
> - Establish a security management structure to assign explicit individual roles, responsibilities, authority, and accountability.
> - Develop plans and initiate actions to provide adequate information security for networks, facilities, systems and information.
> - Treat information security as an integral part of the system lifecycle.
> - Provide information security awareness, training and education to personnel.
> - Conduct periodic testing and evaluation of the effectiveness of information security policies and procedures.
> - Create and execute a plan for remedial action to address any information security deficiencies.
> - Develop and implement incident response procedures.
> - Establish plans, procedures and tests to provide continuity of operations.
> - Use security best practices guidance to measure information security performance.

A one page policy governed the university system from 1992 until 2005. The policy required each unit to develop a security plan that followed USG guidelines. In the early 2000's, the staff of the USG created a number of policies dealing with general

[11] From USG InfoSec/Security Governance page http://www.usg.edu/infosec/security_governance/ accessed 22 Nov 2011

requirements for a security program at each unit. By 2008, the USG policy consisted of 13 separate policy statements and guidelines.

An analysis of those objectives (Table 1-1), broken down by the Carnegie classification[12] for each institution, shows that the Acceptable Use Policy[13] is the only category of security policy for which all USG units are compliant (Table 1-1).

Table 1-1 Distribution of USG Units meeting Requirements per Carnegie Class

USG Policy Requirement	# Compliant	%	AA	% AA	BA	% BA	MA	% MA	RU	% RU
USG Info Sec Policy Section 11 (2011)	26	81%	8	67%	3	75%	10	91%	5	100%
USG Password Authentication Policy	21	66%	4	33%	3	75%	9	82%	5	100%
USG Appropriate Use Policy	32	100%	12	100%	4	100%	11	100%	5	100%
USG Risk Management Policy	11	34%	2	17%	1	25%	4	36%	4	80%
USG Data Handling and Storage Standard	23	72%	8	67%	3	75%	7	64%	5	100%
USG Computer Security Incident Management Policy	13	41%	4	33%	3	75%	3	27%	3	60%
Web Privacy Policy	14	44%	5	42%	1	25%	5	45%	3	60%
USG - HIPAA Privacy and Security Policy	4	13%	1	8%	0	0%	0	0%	3	60%
USG Continuity of Operations Plan	5	16%	1	8%	2	50%	1	9%	1	20%
Use of Cryptography	4	13%	2	17%	1	25%	1	9%	0	0%
Security and Awareness Program	4	13%	2	17%	1	25%	1	9%	0	0%
Electronic Data Disposal	10	31%	2	17%	2	50%	4	36%	2	40%
Copyright Violation Guidelines	14	44%	3	25%	4	100%	4	36%	3	60%

AA – Associate Degree schools; BA – Bachelors; MA – Masters and some doctoral programs; RU – Research University Source: Author's compilation of policy documents

[12] Derived from empirical data on colleges and universities, the Carnegie Classification was originally published in 1973, and subsequently updated in 1976, 1987, 1994, 2000, 2005, and 2010 to reflect changes among colleges and universities. This framework has been widely used in the study of higher education, both as a way to represent and control for institutional differences, and also in the design of research studies to ensure adequate representation of sampled institutions, students, or faculty.
To ensure continuity of the classification framework and to allow comparison across years, the 2010 Classification update retains the same structure of six parallel classifications, initially adopted in 2005. They are as follows: Basic Classification (the traditional Carnegie Classification Framework), Undergraduate and Graduate Instructional Program classifications, Enrollment Profile and Undergraduate Profile classifications, and Size & Setting classification. These classifications provide different lenses through which to view U.S. colleges and universities, offering researchers greater analytic flexibility.
These classifications were updated using the most recent national data available as of 2010, and collectively they depict the most current landscape of U.S. colleges and universities.
(last accessed 1 Jun 2012)

[13] The words "Acceptable" and "Appropriate" are used interchangeably by organizations and researchers

I observed much of the policy process as an employee of the University System Office. That office provides the staff to develop and implement policies approved by the Board of Regents. Actors from each unit of the University System were engaged as part of the policy process. Efforts were made to create policy for which a consensus from the individual unit representatives could be achieved. While obvious differences in size and mission could explain some differences, I found the disparity in the implementation of policies within classes of similar campuses puzzling, especially given the consensus that preceded Board adoption of the policy.

Ostrom warns us that "conditions can be so diverse that, depending on context, sets of rules that work best in one circumstance may fail in another" (E. Ostrom 2005, 274–276). The information security literature generally agrees that policies must be "tailored" to be effective (Neil Francis Doherty, Anastasakis, and Fulford 2011). Tailoring a policy to be effective for that organization requires efforts to align security strategy, goals, and norms with existing organizational norms, processes, and structures (Bohme and Kataria 2006). The context within for which those policies are developed includes factors, both internal and external, identified within the Knapp model. In general, one might assume that the external factors, with the exception of external threats, would be fairly similar for all USG units as they are subdivisions of a large, constitutionally created, governance body. External threats, as a number of studies suggest, will vary according to the number and types of targets each unit presents. Those external threats may indicate, or cause to bring attention, to organizations that impose requirements via standards. For example, the Payment Card Industry (PCI) has a

set of standards that any organization must follow in order to accept credit cards as payment. The U.S. Government has created a number of standards that an organization must follow if that organization meets the criteria set by the law.

Within units of similar size and mission, the expectation of finding similar policies across similar units should increase as suggested by findings within the research areas of organizational theory and information security. However, other internal factors such as structure and culture do vary among USG units. Perhaps the strongest example of the "diversity of conditions" noted by Ostrom is that of the cultural value of academic freedom. The direct effect of academic freedom on the design of information security is perhaps the most cogent reason that explains why enforcement of rigid, one-size fits all policies is more problematic for higher education organizations (Drevin, Kruger, and Steyn 2007).

Academic freedom is just one of a number of values and norms that constitute culture for USG units. The autonomy of colleges and departments is a significant feature of university governance structure (Blau 1994). The autonomy of UGA colleges and departments is one factor that contributes to a process that takes up to 2 years for policies to be developed.

Autonomy extends to the individual level of analysis. One USG unit security official notes that the aversion of individuals to "being told what to do" creates a structure that writes policy as a "recommendation" as to what to do.

An organization's propensity towards risk and the nature of their IT resource also affect overall policy effectiveness (Rezgui and Marks 2008). The Chief Information

Security Office of Georgia Tech explains how they manage what is an issue of compliance with USG policy with a view towards risk:

> *"…because the centralized organization does not control the budgets within the departments, we put in the policy some business continuity kind of statements and then the procedures and guidelines to follow. And, basically we leave it up to the units to determine how much infrastructure they want to maintain locally. If you decide to maintain local infrastructure, then you have to include business continuity and our internal auditors do audit for that. So, they get to determine their threshold when it comes to infrastructure continuity. We just set the top level policy and what continuity should look like."*[14]

A number of organizational factors affect the development of policy and those factors vary from one USG unit to the next. How strongly top management supports efforts to make individual stakeholders aware of the consequences of ignoring policy is one factor noted in the evidence gathered for this study. Stakeholder perception of risk, coupled with the effectiveness and/or presence of awareness and training programs, interact with individual user perception of top management support to affect the policy options considered as "realistic" by policy makers. The structure of the policy process is affected by "who" is at the table as well as "what" those at the table may do. And, the concept of collaboration plays a role in the effectiveness of the policy processes observed. Each of these concepts reveals various tensions among stakeholders and their individual and aggregate sets of values and norms.

[14] Baines, Herb. (22 March 2012) Telephone interview.

1.4 Purpose and Plan of Research

This study has three objectives. First, at the theoretical level, I seek to add to the body of knowledge concerning the relationship between the structure of cybersecurity policy processes and the outcomes of those processes. Second, at a methodology level, the study seeks to demonstrate the usefulness of the IAD framework and tools to discover and define the structure of cybersecurity policy processes and the policy documents produced as outcomes. Third, at the practical level, the study seeks to provide pragmatic suggestions for cybersecurity managers and university executive management to identify deficiencies in cybersecurity governance that contribute to less than optimum outcomes.

Since no integrative framework exists for describing or predicting how organizations adopt and implement cyber security policy (Hsu, Lee, and Straub 2012, 919), this study constructs one by merging concepts from relevant fields of study. Chapter Two examines theories of the policy process as I lay out my case for choosing the Institutional Analysis and Design framework to systematically explore the relevant features of policy processes employed by universities to create and implement security policy. The analysis of competing theories and frameworks concludes with a description of the complimentary features of the Knapp governance model and the IAD framework. In chapter 3, I identify a number of hypotheses to be tested from among the findings and theories discussed. These hypotheses reflect Whitman's challenge to "examine what organizations do to adapt these policy frameworks and models to achieve effectiveness within their particular environments (2008, 147)."

The case study method is appropriate for exploring a question that attempts to explain "how" policies are developed within USG units. Chapter 4 elaborates on the research design and methods used to collect, aggregate, and analyze the data. In particular, I will outline the contributions of the institutional grammar tool as proposed by Hess and Ostrom (1995) and expanded by others (Basurto et al. 2010a; S. Siddiki, Basurto, and Weible 2012; S. Siddiki et al. 2011; Weible, Siddiki, and Pierce 2011; Carter et al. 2013; Carter et al. 2015).

Chapter 5 presents the context for the cases as defined by external factors identified by my interviews as most influential upon the governance structure for each case. A discussion follows of the context of each case and how the external conditions are linked to the case summary. The chapter discusses the utility of IAD descriptors to categorize and identify the key features of the standards and the context of each case.

I separate the findings into two chapters. Chapter 6 discusses the findings relative to a set of hypotheses designed to understand the link between varying external conditions and the structure of cybersecurity governance found in each case. The relationship between the defined policy structure and the governance structure is analyzed. Chapter 7 analyzes the structural details of the four action situations that are responsible for implementing the cybersecurity policies created by the case governance structures. These processes represent the administrative systems engaged in implementation and the institutions that regulate individual behavior within those systems. Chapter 7 answers the question of whether the IAD tools can identify the

patterns of interaction Robichau and Lynn thought critical to describing the "missing link" between policy and performance.

Chapter 8 is a discussion of how the structure of cybersecurity policy processes affects policy structure and the management practices observed. Chapter 9 offers a discussion of this study's contributions to theory, method and practice and possible directions for future research.

Chapter 2- Policy Processes, Governance, and Structure

Chapter 1 presented an overview of research in the field of information security that points to a gap in the understanding of processes employed to design and construct policy and management practices. Researchers find that security policies implemented in higher education organizations are not likely to be tailored to fit the university's , or college's, unique environmental and organizational contexts (Neil Francis Doherty, Anastasakis, and Fulford 2011). Tailoring is a process that seeks to "fit" the rules, norms, and standards that define policy to the features of the problem for which the policy is meant to regulate (Bohme and Kataria 2006). Information security governance is thought to be most effective when the essential policies processes suggested by Knapp, et al. (2009) are designed to work within the constraints posed by the particular internal and external influences of an organization.

Studies involving institutions and the governance of shared resources often reference Garrett Hardin's "Tragedy of the Commons" (1968). The idea of how to prevent the "over grazing" of a public commons is often described as a simple, straight-forward discussion of how private behaviors may best be incented to avoid an outcome that negatively affects everyone. Similarly, much of cyber security policy focuses on incenting individuals to avoid bad choices that can compromise the integrity and reliability of the information and technology to which those individuals have been granted access. For example, using computers on a university network to store and distribute illegal copies of movies takes bandwidth and computing power (i.e. the

common pasture) away from students and employees that need to use for legitimate purposes. The failure to maintain anti-virus software may allow denial of service attacks that will shut down a university network as the bandwidth is consumed by those attacks.

A re-examination of the premise of Hardin's article suggests that most approaches to 'problems of the commons' oversimplify the analysis of the phenomenon (Cole, Epstein, and McGinnis 2014). A rigorous analysis requires an understanding of how well the institutions: 1) fit the internal and external conditions of the problem, and 2) fit the existing institutions (2014, 10).

In the next section, I review the concept of governance and policy making within the information security literature. I follow with a brief overview of the IAD framework and how the concepts of collaboration, governance, and culture contribute to that framework. The synergies identified between the fields of institutional analysis, policy governance, and information security provide strong arguments to support the research model created by integration of the IAD framework and the Knapp model for information security governance. The ability of the research model to address the challenges identified by Robichau and Lynn is a matter to be determined by the outcomes of this study. A summary of the arguments presented closes the chapter.

2.1 Governance – Institutions and Implementation Research

The concept of institutions is essential to theories of economics, political science, public policy, sociology and others (Coleman 1986). Institutions fundamentally

determine how organizations come into being and evolve (North 1990, 5). Institutions are observed as "rules, processes, norms, and strategies employed by humans to organize their work, their social relations, and their life; in sum to manage human behavior" (E. Ostrom 2005). Analyzing institutions helps researchers in their quest to understand what Ostrom characterizes as "one of the most fundamental political and social questions: How do fallible human beings come together to create communities and organizations, and make decisions and rules in order to sustain a resource or achieve a desired outcome?" (E. Ostrom and Hess 2007, 42).

O'Toole (2000, 266) defines implementation research as "the development of systematic knowledge regarding what emerges, or is induced, as actors deal with a policy problem". Specifically, he defines policy implementation as "what develops between the establishment of an apparent intention on the part of government to do something … and the ultimate impact in the world of action" (2000, 266). Analysis of policy implementation often involves two questions: 1) why are adopted policies not as designed; and 2) why are the outcomes not as we expected (Elmore 1979)?

Understanding and explaining the difference between "policy as designed" and "policy as implemented" is important for those interested in policy implementation and organizational management (Imperial 2005). O'Toole's assessment of implementation research suggests that efforts involving the concepts of institutional analysis, governance, and networks, taken all together, are making substantial contributions to understanding the outcomes of implementation processes (2000).

2.1.1 Policy Governance

The policy studies literature is populated with diverse meanings that are "imprecise, [and] wooly" (Fredrickson 2005, p. 289 as found in Robichau 2011). While researchers agree that both policy makers and evaluators must consider how governance affects the implementation process (Jochim and May 2010; R. P. Stoker 1991; G. Stoker 1998; Stone 1998; Meier 2009a), there is a significant gap in this area of knowledge (Weible and Carter 2015). Within the higher education research genre, research has found different governance structures may lead to similar outcomes (Lowery 2002). Critics note the field has produced "few theoretically valid and methodologically reliable approaches … to assess policy divergence as it occurs during the policy process" (Carter et al. 2015, 159).

The information security literature defines information security governance as the incorporation of security policy in alignment with the corporate governance structure and its strategic plan (Posthumus and von Solms 2004, 643). The Knapp model defines the concept as inclusive of a number of related processes required to "govern" information security issues within an organization. The processes that review, develop, and align policy with organizational governance are important elements of the policy governance structure that this study analyzes.

Networks of actors, processes, and institutions are common themes found in the areas of research upon which this study rests. Multiple frameworks have evolved that analyze the concept of networks applied to governance. I explore three such frameworks in this section. O'Toole and Meier propose a framework focused on

management quality , and management networks, as a means of explaining the variance in policy outcomes (O'Toole Jr. 1997; Laurence J. O'Toole and Meier 2004). Lynn, Heinrich and Hill propose a "logic of governance" linking collective action with observed factors of influence (Lynn, Heinrich, and Hill 2000). The criticisms of each approach provide a transition to the discussion of the IAD framework as a means to carry the work forward.

2.1.2 Policy Networks and Governance

Managing coalitions and managing institutions are key to understanding how policy networks are effective in managing public problems (Meier 2009b). Policy networks have been suggested as a feature of governance structure that facilitates the sharing of resources, the collaboration of multiple parties to obtain shared goals, and the creation and exchange of knowledge (Weber and Khademian 2008). In order for policy networks to deliver those described outcomes, managers must have the proper tools and skills to build "long-term collaborative problem solving capacity" (Bardach 1998; E. Ostrom 1991; Provan and Kenis 2008; Meier and O'toole 2001).

O'Toole explains that individuals "can be seen simultaneously as occupants of positions within a public administrative organization and also as one component of a multi-organizational web of action … focused on a function or public problem" (2010, 8). Networks do not necessarily replace the hierarchy as the functioning structure of an organization but, rather, complements, overlaps and even competes with the existing hierarchical structure. The challenge, O'Toole notes, is the use of appropriate authority to coordinate and manage the action within and across these structures.

Network-based collaborative action may spring from "voluntaristic, self-organized, and consensual" efforts (Ostrom 1990 as cited in O'Toole 2010). Adding network actors to the public management context both adds capacity and complications as regards the goals meant as constraints on action (Simon 1964) and transparency (i.e. who is doing what to whom)(O'Toole 2010). O'Toole suggests research is needed to understand how network structure and efforts to manage the networked array influence outputs and outcomes (2010, 10).

"Wicked problems" represent a category of policy challenges that cut across problem areas, policy domains, and authority structures within and across organizations (Weber and Khademian 2008). DeLeon and Varda (2009) offer collaborative inter-organizational policy networks as the preferred structure of governance required to manage wicked problems. Others suggest that the nature of wicked problems requires management by collective action (van Bueren, Klijn, and Koppenjan 2003) as wicked problems are such that "no single organization can act with assurance of predictable outcomes (Westley & Vredenburh, p. 381 as cited by deLeon and Varda 2009). These collaborative policy networks would need to focus on:

- efforts to draw on a broad range of knowledge,
- a base of knowledge to address the complexities of the problem,
- serving as a means of cooperation
- maintaining efforts to transfer, receive, and integrate knowledge as dimensions of the problem will change and the participants (i.e. managers) of the problem will change as time progresses. (Weber and Khademian 2008, 337)

But, collaboration is not necessarily an activity free from friction. Implementing policy within a university requires the collaboration of the various units of university,

with different missions and objectives. Collaboration also requires the support of individual actors.

> "The study of multi-actor policy implementation needs a theoretical approach that combines the self-organizing potential of combinations of actors (including corporate actors) with the mandated character of certain inter-unit links, the latter quite typical of at least some portions of government programs." (O'Toole Jr. 2000, 275).

2.1.2.1 Governance and Managerial Networking

1.1 The work of Meier and O'Toole investigates how the quality of public managers influences public performance. They investigate whether managers, by interacting with their networks, contribute to the performance of their respective jurisdiction (Meier and O'toole 2001). Meier and O'Toole explore the question of whether the efforts of public managers within their networks, which extend to other organizations outside their jurisdiction's hierarchy, affect the performance of their organization. Networks allow managers an opportunity to understand the interaction of policy with environmental factors and to prepare strategies to mitigate those factors and optimize performance. Among their findings: network management allows managers to translate resources into outputs at a more efficient rate; and performance improves in districts where managers engage in more network interactions.

> "Networks are structures of interdependence involving multiple organizations or parts thereof, where one unit is not merely the formal subordinate of the others

in some larger hierarchical arrangement (O'Toole 1997, 45 as cited in (O'Toole Jr. 2010, 8))."

This concept of networks has many similarities to the concept of sub-parts that Simon (1962) described. Both concepts emphasize that these sub-parts, while a part of a larger organization, do not necessarily confine themselves to the hierarchy of a given organization, nor, as an inter-organizational entity, to the boundaries of a given organization. O'Toole explains that individuals "can be seen simultaneously as occupants of positions within a public administrative organization and also as one component of a multi-organizational web of action … focused on a function or public problem (O'Toole 2010 8)."

Networks do not necessarily replace the hierarchy as the functioning structure of an organization. Networks complement, overlap and compete with the existing hierarchical structure. The challenge is the use of appropriate authority to coordinate and manage the action within and across these structures (O'Toole 2010 8).

Network-based collaborative action may spring from "voluntaristic, self-organized, and consensual" efforts (Ostrom 1990 as cited in O'Toole 2010). Adding network actors to the public management context both adds capacity and complications as regards the goals meant as constraints on action (Simon 1964)) and transparency (i.e. who is doing what to whom)(O'Toole 2010 8).

2.1.2.2 Logic of Governance

The logic of governance (LOG) approach is a framework, not a theory, offered as a means to organize findings of empirical research, developed by multiple and diverse

communities of researchers, on various aspects of public governance problems (Heinrich, Hill, and Lynn, Jr. 2004). A positive outcome of a logically combined effort would allow public management researchers to offer answers to the question "How can public sector regimes, agencies, programs and activities be organized and managed to achieve public purposes (Lynn, Heinrich, and Hill 2000). The model organizes studies of governance in relation to their position in a set of hierarchical interactions starting with public preferences, as expressed by political and legislative choice, and extending through stakeholder assessments. Operationally, the authors offer a reduced form of their proposed model:

$$O = f(E,C,T,S,M)$$

Where:

E = environmental factors
C = Client characteristics
T = treatments
S = structures
M = managerial roles and actions

The logic model acknowledges the multi-level characteristic of public governance and the discretion by managers to implement policy as they wish (within constraints). Researchers benefit from such a framework as they would have access to more details of effects that are exogenous to their particular research focus and thus can model those effects across there area of research (Lynn, Heinrich, and Hill 2000, 247).

2.1.2.3 Criticisms of the LOG approach

Lowery (2002) criticizes the focus on "one narrow dependent variable" that reduces the study of public governance to questions of governance and public sector outputs. Lynn-Heinrich-Hill (2002) respond by arguing "isn't performance what the

public cares about?" Lowery points to Simon's *Architecture of Complexity* (1962)as a theory that argues for analysis of hierarchical organization as a reduction to its "decomposable parts". Lynn-Heinrich-Hill say that Lowery misunderstands their thesis and that the framework does not disallow Simon's concepts (2002).

Lynn, Heinrich and Hill acknowledge the existence of alternative frameworks for studies of governance that may be more appropriate given the research question or context or the proposed unit of analysis (p. 241). For example, the LOG focuses on the individual as the unit of analysis relying on institutional political economy to guide questions as to why an individual chose certain paths. Their review of the literature points to network analysis as a logic that explains implementation and performance based upon social and political relationships among various organizations (actors) with varying interests and resources. The exchange of information among network members explains the network's influence on outcomes as the network optimizes the promotion of individual actor's interests (p. 242).

2.1.3 Governance and Institutional Analysis and Development

The Institutional Analysis and Development framework (IAD) has been employed to understand phenomenon such as collaboration and its role in the implementation process (Buchan et al. 2009), the role of institutional settings in the implementation process (1999a), strategies required for adaptive governance (Koontz 2005), and the analysis of the effects of globalization upon cooperation (Clement and Amezaga 2008). Carlsson (2000) proposed integrating the policy network approach into the IAD framework taking advantage of the IAD's analytical tools "to examine the processes of

policymaking". Others promote the framework as one appropriate to understand questions of governance in areas of study beyond that of common pool resource problems (Nowlin 2011). This study takes advantage of three strengths of the IAD approach: (1) the success of modeling approaches to successful governance of common-pool problems; and, (2) the relevance of identifying and mapping configurations of institutions and actors as the structure of policy governance; and, finally, (3) the ability of the IAD to integrate research from multiple disciplines.

The framework has been applied to a number of studies of governance related to managing common-pool resource problems. Contributions from the study of natural resource problems relevant to the governance of cybersecurity are numerous. The application of IAD to the university knowledge ecosystem is particularly relevant to this study (E. Ostrom and Hess 2007). The authors propose that "conceptualizing information and knowledge as a commons brings a rich body of research on natural resource commons to the table" (Hess and Ostrom 2004). Information technologies such as networks, servers, and databases, are facilities that have limits to capacity, to which access is restricted (e.g. club good), and for which the consumption of the resource by one denies that resource to another (rivalry) (E. Ostrom and Hess 2007).

Smith (2010) employs the IAD framework to analyze "institutional arrangements used to implement ecosystem-based management programs". He argues that in order to implement key principles for ecosystem management, policy makers must focus on questions of institutional design and performance. His study finds that "polycentric

institutions can be just as effective as centralized hierarchical approaches to coordinating and implementing integrated coastal resource management programs".

Koontz (2008) examined several counties in Ohio to determine how collaborative planning affected the implementation of land-use policies. He found that local context affects collaborative efforts. Collaboration fails to yield expected outcomes if the context (i.e. local rules/institutions) is not conducive to collaboration. Clement and Amezaga (2008) demonstrate how the conflict in values, and structure, between national land use policy institutions in Viet Nam and local institutions, where there is a high degree of individual interaction, created turmoil in the implementation of the policy. Stable institutions and governance structures that facility collaboration contribute significantly towards building trust and credibility among the actors networking to achieve open-space protection. Mollenkamp and others (2008) compare two different agencies responsible for implementing water management policy and find differences of power, as exhibited in decision-making processes, led to different implementation outcomes for the same policy.

The second strength of the IAD framework relevant to this research project is the focus on configurations of institutions and actors as integral components of the implementation process (McGinnis 2011b). There are institutions of governance that affect organizational learning, especially the institutionalization of knowledge and values within a given organization or system (Blomquist and Ostrom 2008; Anderies, Janssen, and Ostrom 2004; Hess and Ostrom 2004). The identification of such configurations (Basurto et al. 2009; S. Siddiki, Basurto, and Weible 2010; Carter et al.

2013) contributes to a reliable method of studying the relationship between policy processes and policy outcomes (Kwon, Berry, and Feiock 2009; Weible and Carter 2015). Mapping the structures of policy processes (governance) and policies (outputs) contributes to the identification of patterns in outcomes (Aligica 2006). As to policy management, "stakeholder mapping and institutional mapping are indispensable strategic instruments (Aligica 2006, 76).

Finally, the ability of the framework to integrate findings across multiple disciplines is key. The use of the framework and its tools have expanded beyond the study of areas traditionally tied to common-pool resource problems. The mission of the Ostrom Workshop is "to build upon the theme of governance to understand and address major societal problems"[15]. Scholars expect that the "utility of the framework is likely to be both further demonstrated and further improved" as IAD applications extend to examine institutional structure in areas "from securities trading to academic tenure" (Blomquist and deLeon 2011). Scholars have suggested tying the IAD framework with the Advanced Coalition Framework in efforts to better understand the structure of belief systems and how key actors attempt to modify that structure for various purposes (Weible et al. 2011) . The framework has been applied to study how institutions evolve in judicial systems (Blomquist and Ostrom 2008). Scholars are using the framework to better understand structural diversity expressed via city charters and how the various structures affect public participation (Feiock et al. 2014).

[15] "Research Mission", The Ostrom Workshop Indiana University Bloomington, accessed 31 October 2015, http://ostromworkshop.indiana.edu/about/mission.php

Robichau and Lynn suggest that the IAD framework holds considerable promise to expand and explain concepts of networks and governance in terms of relationships between administrative systems and processes that extend beyond the concept of institutions (2009, 30). But, the condition their suggestion noting that the IAD approach may be challenged to interpret "patterns of interaction" involving policymaking structures, management structures, processes, and outputs are interpreted as "patterns of interaction" within and among action situations. Of course, it this the interaction among the various processes and structures that Cole et al. (Cole, Epstein, and McGinnis 2014) argue must be understood. Identifying the effects of these patterns is a way forward on the "missing link" of implementation research, the focus of Robichau and Lynn's analysis.

2.1.3.1 Levels of Analysis

The IAD framework provides a systematic analysis of the structure of situations where choices must be made. That structure is defined by the institutions involved, and the individuals and communities affected (E. Ostrom 2005, 9). Figure 2-1 illustrates the working parts of institutional analysis. Three levels of decision-making define an arena where actions are taken and outcomes produced via multiple, nested action situations (Kiser and Ostrom 2000). The three action levels of operational, collective, and constitutional choice reflect the nested nature of governance prevalent in polycentric systems (McGinnis 2011a, 173).

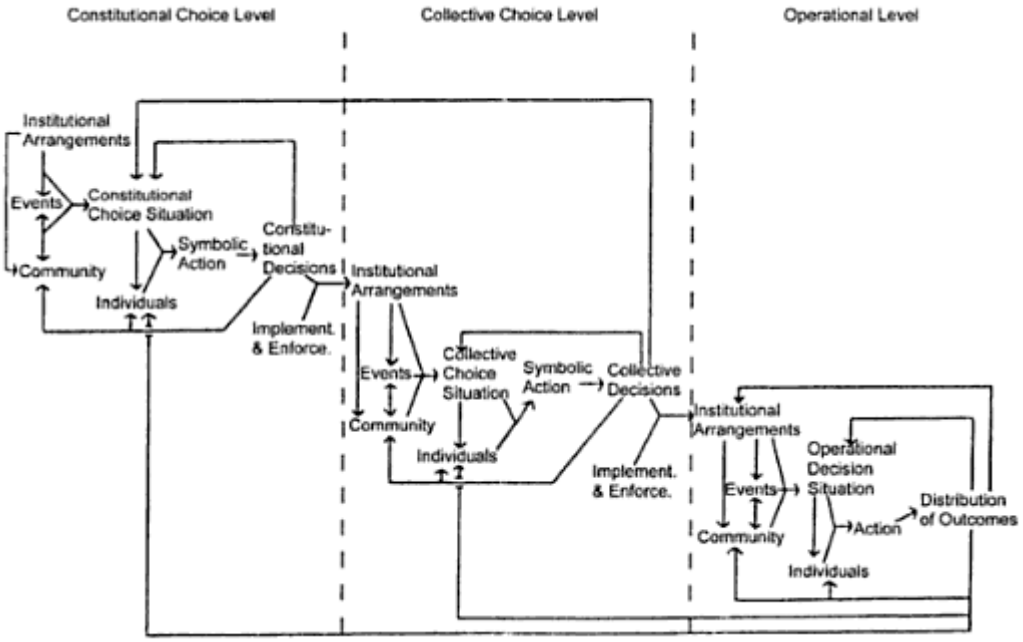

Figure 2-1 Three Levels of Institutional Analysis
(Source: Kiser and Ostrom, 2000, p. 60)

Those distinct levels of choice also represent distinct levels of analysis. The Operational Level is described as "the world of action"(Kiser and Ostrom 2000, 76). Actions at this level "involve the day-to-day actions of individuals working with the resource" (Hardy and Koontz 2009). Analyses at this level focus on the choices made by individuals regarding actions allowed by decisions at the collective choice level (McGinnis 2011a, 173). In our examination of cyber security policy, polices that define how students, staff, and faculty may use campus technologies are categorized as operational level rules. For example, one form of acceptable use policy is one requiring individuals to install anti-virus software on their computers prior to connecting to campus networks. The individual user must comply with the rule or be sanctioned,

possibly by an automated refusal to allow their computer to connect to the campus network.

Individuals, i.e. users and managers, need accurate information that helps them to understand the benefit of compliance, and, the risk of non-compliance (E. E. Anderson and Choobineh 2008; R. Anderson and Moore 2009). In the world of micro-institutional analysis, management practices (e.g. policy enforcement and training), rules and norms (i.e. policies) are institutional arrangements created from a combination of collective level decisions (policies) and organizational culture (Kiser and Ostrom, 2000, 76). The decisions made at this level result in an action that affects the resource (cyber space). Such actions may include a user's decision not to install anti-virus software, or management's decision not to enforce a policy. Such decisions will lead to a deterioration of the resource.

Collective Choice level decision-making includes "the processes by which institutions are constructed and policy decisions made, by those actors authorized to participate in the collective decisions as a consequence of constitutional choice processes, according to the procedures as established by constitutional choice processes" (McGinnis 2011a, 173). The outcomes from the decisions made by actors at this level combine to create plans for the execution of operational level actions (Hardy and Koontz 2009). Factors such as alignment of business objectives, culture, economic factors, and the structure of cyber security governance affect the actors and outcomes of this level of action (Knapp et al. 2006).

The outcomes from the Collective Choice level include rules that enable, or prohibit, a key management practice; rules that require or forbid a specific action to be taken by a user of computer services, and so on. Collective Choice rules determine the resources available for training and awareness, incentives for adoption of certain policies, and who has ultimate approval of policies under consideration. In other words, decisions made at the collective choice level "… determine, enforce, continue, or alter actions affected within institutional arrangements" (Kiser and Ostrom 2000, 77).

Constitutional level decisions affect the decision rules that constrain the collective choice level decisions (Imperial 1999b). Rules created at this level may determine who participates in making policy, what options may be considered, and who is held accountable for the outcomes generated at the collective level (Hardy and Koontz 2009). The Board of Regents policy manual is one source of constitutional choice rules identified for our study. Federal and state mandates provide additional constitutional choice rules.

2.2 Mapping Governance Concepts with the IAD Framework

Robichau and Lynn (2009) suggest that process modeling, utilized in public policy theories, and multi-level analysis may enhance the strength of governance theories. Their analysis of policy theories included in Sabatier (2007b) found two areas of concern: " the failure to distinguish between outputs and outcomes and the imprecise treatment of the role of administrative systems in mediating the relationship of policymaking to its ultimate consequences (p. 27)." Noting the similarities between

Ostrom's IAD framework and the LOG framework, they suggest Ostrom's framework be expanded to include "more discussion of the relationships of administrative systems to structures and processes beyond rules (p. 30)".

A challenge to any form of institutional analysis is the need for a methodical means of examining cases to search for factors relevant to the outcomes produced (Aligica 2006, 71). Aligica posits that "an outcome consistent with a pattern may be the best verification we can achieve in settings of substantial complexity (Ostrom 2005 11 in Aligica 2o14). Identifying such a relationship addresses the missing link problem.

2.2.1 Information Security: Governance, Frameworks and Models

Hong (2006), May and Dhillon (2010), and Knapp et al. (2007; 2009; 2006), discussed in the previous chapters, describe efforts to conceptualize theories and frameworks to study the human and organizational elements of cyber security. These and other studies (Appari, Johnson, and Anthony 2009; D'Arcy and Hovav 2008; Hassebroek 2007; Hu, Hart, and Cooke 2007) indicate a positive contribution from research examining institutional factors of policy processes and cyber security. Bjork (2004) suggests that research engaging institutional theory will enhance research into policies designed to secure cyber assets via the management of human behavior.

Hsu, et al, did not find an "integrative framework depicting how organizations adopt and assimilate administrative innovations in response to institutional pressures" (2012, 919). Numerous efforts have examined various components, or factors, important to understanding how organizations adopt and implement policy and the practices that are necessary to maintain successful policy. The paper concluded that

future research regarding the “interaction between institutional pressures and organizational change” would be important in efforts to understand the traits of effective information security management (p. 936).

The literature clearly identifies a number of processes and factors that interact with institutional arrangements to affect processes that develop, adopt, and implement security policy. Karyda, et al (2005) describes the policy process as one of inputs, activities, and outputs as embedded in social processes unique to the organization. In order to understand the outputs and outcomes of these processes, one must understand the organizational context. They identified a number of factors they believe merit further research including: organizational structure, the role of an information security officer, participation by users in the policy process, top management support, and training and education (p. 257). Other elements of organizational context include culture, environment, social, political, economic, and technology factors (Hatch 2006).

May and Dhillon proposed a semiotic framework to provide a holistic and general means for addressing the social and technical perspectives of information security (2010). Their framework (Table 2-1) accommodates analysis via six layers of abstraction that focus on categories of signs, basic units of communication, by which information is communicated throughout a community, organization or culture (p. 3-4). Among their findings, Dhillon and May suggest that the framework's systematic analysis of the human, social and technical layers yielded "an enriched security analysis" with implications for more robust security policies (p. 13).

Table 2-1 Semiotic Framework for Security Research

Semiotic Layer	Brief Description	Information Security Issues
Human Level		
Social	System of Norms, beliefs, expectations, commitments, law, contracts, values, shared models of reality, and attitudes	Alignment of mission of business, ethical environment, social implications, and security policy, with security requirements
Pragmatic	Culture, communications, intentions, and negotiations	Organizational norms and security culture; education, training and awareness
Semantic	Meanings and consequences of human behavior	Consequences of misinterpretation of data or misapplication of rules; responsibility and attribution of blame
Technical Level		
Syntactic	Rules, procedures, structure, and language	Software; Security reviews and audits to ensure data integrity and to handle program bugs and software piracy
Empiric	Statistical behavior, efficiency, and redundancy	Telecommunication equipment and network strategies; Virus handling and encryption
Physical	Physical Domain	Hardware; Physical security

Source : May and Dhillon (2010) (Adapted from: Stamper, 1973; Liebenau and Backhouse, 1990; and Dhillon, 1997)

Hong and others offer a conceptual paper that integrates five information management theories (Table 2-2). Individually, these theories fail to account for all the security management activities thought to be essential to effective management (p. 246-7). Reasons for failure include:

- Four of the theories, contingency theory is the exception, emphasize a top-down approach
- Structured methods difficult to adapt to dynamic environments
- Information Security auditing not addressed appropriately making evaluation of policies difficult to do reliably.
- Management systems could not complete periodic cycles.
- Contingency theory lacks comprehensive methods and procedures.

The synthesis proposed by Hong, et al, recognizes the cyclical nature of management activities; the need of a feedback loop for evaluation and modification of policies; and, that management and policy activities are functional processes whose

inputs and outputs create sequential activities. Finally, security management must align with organizational objectives.

Table 2-2 Five Management Theories Adapted from Hong, et al 2003, p. 246

Theory	Mgt Activities	Mgt Procedures	Characteristics	Source
Security Policy theory	Security policy establishment Policy Implementation and maintenance	Sequential Periodic	Policy is main focus Emphasize sequential, structured procedures	Flynn Gupta et al. Kabay
Risk Mgt Theory	Risk Assessment Risk Control Review and Modification	Sequential Periodic	Understand insecure environments Ignore security policy and information audit mechanisms Overemphasize structures	Luthans Wright
Control and Auditing Theory	Establish Control Systems Implement Control Systems Information Auditing			ISO/IEC 1779 COBIT
Management System Theory	Security Policy Establishment Establish Security Scope Risk Management Implementation	Sequential	Information auditing is ignored and implementation is affected Lack of periodic check Lack of feedback	BS7799 Schultz et al.
Contingency Theory	Policy Strategy Risk management strategy Control and Audit Strategy Management System Strategy	Contingency	Consider environments both outside and inside the organization Choose appropriate security strategies	Drazin et al Kaplan Lee et al. Tudor

2.2.2 Cyber Security Policy Process: External and Internal Factors

No single factor has been shown, by itself, to affect cyber security (Neil F. Doherty and Fulford 2006; Kankanhalli et al. 2003a; von Solms 2005; Ku, Chang, and Yen 2009). Studies point to the need of a holistic approach, integrating policy and management practices to incorporate the human, organizational, and technical tools in a dynamic process responsive to a dynamic threat environment (Werlinger, Hawkey, and Beznosov 2009; Easterby-Smith 1997). Flexibility, responsiveness, and sensitivity to context are attributes of a policy process deemed necessary for dealing with a wicked problem, especially within emerging organizations (Baskerville and Siponen 2002). A number of studies suggests that the likelihood of effective cyber security can be predicted by top management support for the organization's information security

program (Fulford and Doherty 2003; Hawkey et al. 2008; Knapp et al. 2006; Warkentin and Johnston 2008).

Threats, both internal and external, constantly evolve. Changes in threats necessitate continual evaluation of risks. Evaluation of the costs of implementing, monitoring and enforcing policies is a constant task. Cyclical evaluation processes indicate an organizational culture, along with management support, to prioritize the organization's efforts to secure its cyber assets. Effective organizational responses to threats depends on the "quantity and quality of information available to decision makers about threats, vulnerabilities, potential damages and likelihoods, the modularity, interdependence and integration of systems, and the scope of responsibilities and risk tolerances of decision makers" (Tversky and Kahneman 1986).

Conflict with business objectives and organizational culture create issues for policy implementation. The requirement of open environments for research and knowledge exchange, thought necessary to protect academic freedom, represents a challenge for practitioners on campuses of higher education (Hawkey et al. 2008). Academic freedom is argued by some in support the decentralization of IT management and IT security management; giving control of IT policy to individual schools and departments. Yet, decentralization may harm efforts to protect organizational information assets. Finally, the interaction of some factors – such as individual variation of perception of risk and the distribution of security information to individuals via a distributed management system – may affect the scope of policy as risk and perceived

costs affect the analysis of cost and benefits (Werlinger, Hawkey, and Beznosov 2009, 13).

While investigating the implementation quality of cyber security controls, researchers find that because of a lack of sufficient knowledge, managers implement as many controls (tools, policies) as possible without regard to the effectiveness of those controls (Wade H. Baker and Linda Wallace 2007). The authors propose that managers should adopt the quality management paradigm: incidents reflect defects in the organization's security program.

Effective cyber security is the implementation of appropriate policies and management practices that yield positive outcomes such as a decrease in security breaches, an increase in blocked attacks, or a measured increase in system integrity (Sangseo Park, Ahmad, and Ruighaver 2010). If an organization can identify the appropriate controls for their situation and implement them efficiently, then the organization can effectively manage information security risks (D. W. Straub and Welke 1998 as cited in Baker and Wallace 2007).

2.2.3 Governance in Higher Education

The literature concerning governance in higher education is quite extensive. I will highlight two findings of importance to this study. The structure of governance and the cultural value of autonomy.

Millett observed that University departments, centers of research, colleges and schools present a distribution of authority that contains hierarchical as well as horizontal lines of authority. (1962, 61)." He describes "communities of power"

organized in four constituent groups: faculty, students, alumni and administration (p. 62). These communities create internal organizations that confound attempts to centrally organize or administrate higher education (p. 62). A school, or college, may maintain functions to manage academic, business, student, and information system needs that are duplicated in other schools and divisions of the university.

The autonomy of colleges and departments is a significant feature of university governance structure (Blau 1994). The influence of autonomy contributes to an organizational structure that Cohen and March (1972) describe as a form of organized anarchy with a policy process best euphemized as akin to producing good eats from a "garbage can". Research into the phenomena of collaboration within institutions of higher education demonstrates how factors such as norms, values, knowledge, experience and autonomy can defer or defeat efforts to collaborate.

A polycentric structure consists of multiple centers of decision-making where authority may overlap yet the interaction of those centers occurs in a consistent manner (Imperial 1999b). Ostrom and Hess (2007, 44) believe analysts should employ a framework that can assimilate the polycentric nature of such enterprises and the multiple levels of analysis required to understand them. This belief suggests a conflict between the hierarchical structure observed by Millet and the polycentric structure suggested by Ostrom as one that "fits" better the cultural value of autonomy.

2.3 Mapping the Policy Process – A Research Model

Peter Blau (1974, 12) defines structure as "the distributions, along various lines, of people among social positions that influence the role relations among these people." This definition has the following components: 1) individuals and interactions among individuals, 2) rules either explicit or implicit (vis-à-vis role definitions) to govern those interactions, and 3) levels of influence (hierarchy). The IAD framework emphasizes actors constrained by rules within a given action situation (E. Ostrom, Gardner, and Walker 1994).

The IAD framework divides the factors that influence a collective-level action situation into three categories: 1) Material/Organizational Conditions, 2) Community Attributes, and 3) Rules-In-Use. I translate the internal influences identified by the Knapp model as community attributes but rename the category as organizational factors. For reasons of parsimony, I rename the category of Material conditions as External Conditions. The relevant factors taken from findings of the information security literature are mapped into the three categories to finish the description of the research model (See Figure 2-2).

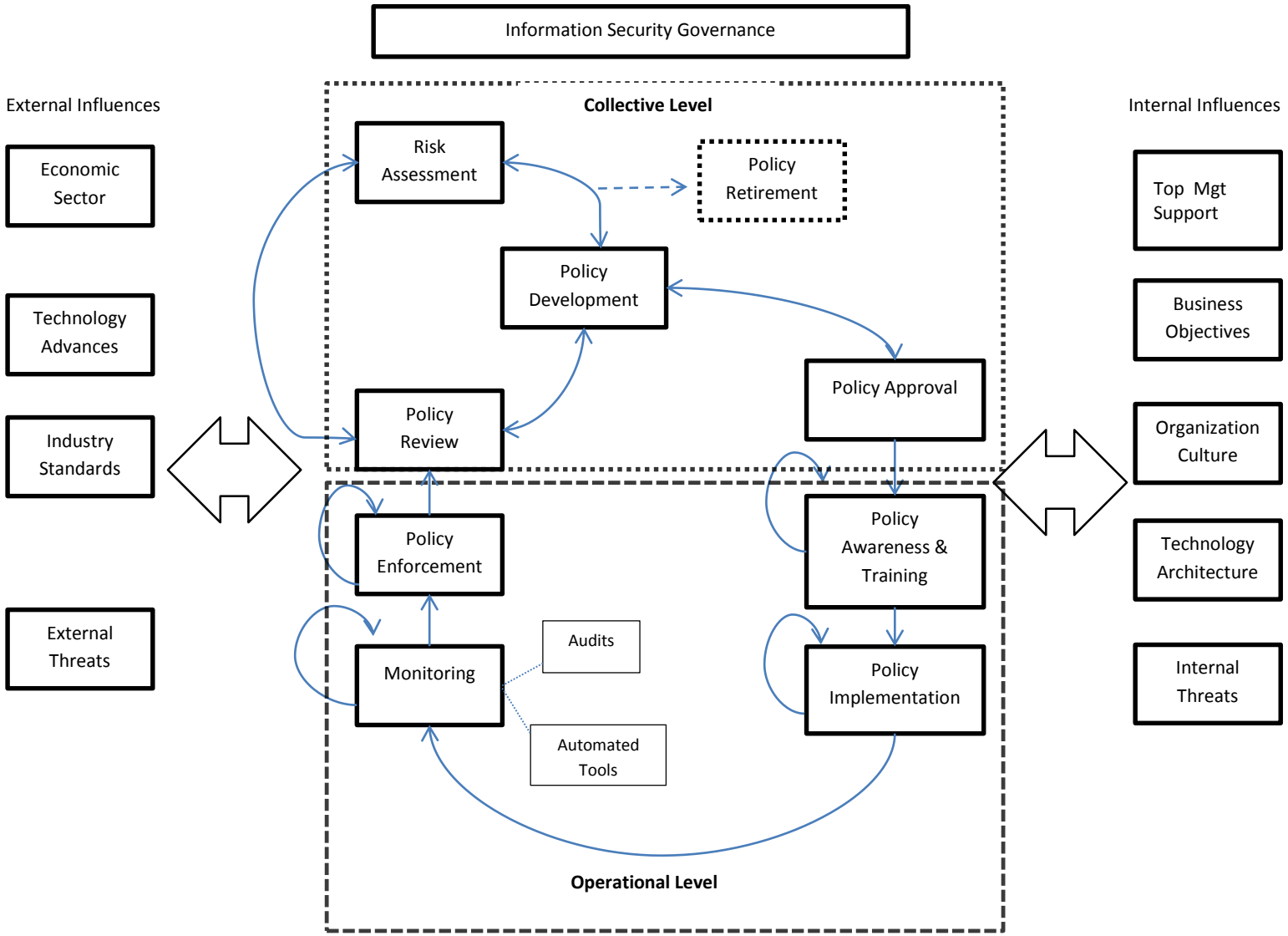

Figure 2-2 Knapp Governance Model as Networks of Action Situations

The processes identified in the Knapp model reside at different and multiple levels of decision-making. I identify the Knapp processes of Risk Assessment, Policy Review, Development, Retirement and Approval with the Collective Level of the IAD model. The processes of Training, Implementation, Monitoring, and Enforcement are placed at the Operational Level. Each level of action interacts with the other levels affecting outcomes, rules modifications, adjudication of differences, and individual decisions of compliance (McGinnis 2011b; E. Ostrom 1990).

How does the research model reflect the context of the cases in this study? The Knapp model maps processes identified by both researchers and practitioners as essential to effective information security governance. The IAD framework can map the features of the structure of these processes both singularly as a solitary action situation or as a network of action situations (McGinnis 2011b). Recall the three levels of choice shown in Figure 2-1. The constitutional level of choice represents the decision-making situation held by the Board of Regents of the University System. The collective level situation represents the policy process for each of the USG campuses. The operational level situation represents the various sub-units, including individuals that are engaged in daily operations that are regulated by the policies created at the collective level.

The Knapp model provides expectations of what an analyst should expect to find in an organization that seeks to implement an effective security policy. In other words, the model is a high-level map of policy processes. The model can be overlaid at any point in the process. For example, an analysis of policy making at the Board of Regents Level would map the processes for collective level decision to the Board and staff

committees responsible for developing and reviewing proposed policies. The "constitutional level" rules applied to the Board would be found in the state constitution as well as statues and regulations from both state and federal government units. If a campus is of sufficient size requiring complex sub-units such as colleges and research divisions, the collective level can be focused at the sub-unit level.

The precision of analysis increases as the analyst drills into the structure of each Knapp process. The IAD model of an action situation identifies, at a minimum, several sets of variables (Table 2-3) that describe the structure of a process: (1) participants, those involved in the process; (2) positions that are associated with a set of actions that the holder of a position is authorized to employ; (3) actions (decision points) for each process; (4) outcomes: results from the interaction of participants determining actions within the rules that constrain such decisions; (5) information: about the process and the implications of potential decisions and outcomes; (6) payoffs: incentives and disincentives for potential actions and behaviors of the participants in the process; and, (7) control: who may make decisions determining outcomes.

Table 2-3 Rule Types

Type of Rule	Regulated Component	Description
Position	Positions	Title of position; Number of actors in a position; quorum level;
Boundary	Participants (Actors)	Define (1) who is eligible to enter a position, (2) the process that determines which participants may/must enter positions, and (3) how a participant may/must leave. Some rules may spell out eligibility for participants
Choice	Actions	what an actor must, must not, may, may not do based upon Conditions at the time of decision - Choice rules affect the total power created in an action situation Choice rules determine the decision tree linking actions to outcomes
Aggregation	Control	whether one individual decides, or votes of several aggregate to decide Determines the level of control an actor given a position may exercise over the selection of an action
Information	Information	Affects level of information available to participants; limits topics to be considered; frequency and accuracy of communication, legitimate channels of communication, language
Payoff	Costs/Benefits	Assigns external payoff/sanctions to particular actions Creates incentives and deterrents for action
Scope	Outcomes	Defines the range of acceptable outcomes permitted. Also limits actions linked to the outcomes.

Source: Adapted from Crawford and Ostrom (2005, 191) and Ostrom (2011)

The configuration of these variables are affected by the organizational and external factors identified in the Knapp model. The framework classifies rules by identifying the component the rule regulates. Configurations of these rules have been suggested as a means of understanding policy change across time and organizations in a "rigorous manner" (E. Ostrom and Basurto 2011). These configurations may identify features of the policy processes employed by each campus and thus define the structure of those processes. The next chapter will elaborate on this point.

2.4 Summary

Relevant theories of the policy process were reviewed and key concepts identified to define and identify structures of policy processes used to develop information security policy. A strong criticism of the theories is that the link between

policymaking and the actions within administrative systems to implement those policies is not explicitly defined (Robichau and Lynn Jr. 2009). The Knapp model presents an approach based on both theory and practice that provides a systematic approach to analyzing and defining those relationships. The utility of the IAD framework to identify these concepts as structures of actors and institutions represents a viable opportunity to address a serious gap in understanding the relationship between policy processes and the divergence of policies implemented from the intended designs. In Chapter 3, I discuss the theoretical expectations of relationships between policy structure and the policy process and several hypotheses that the study will use to test those relationships.

Chapter 3– Hypotheses

The IAD framework and the research model offered by Knapp, et al., both agree that the influence of external and organizational conditions affect and regulate the behavior of the decision making within the action situations being studied. I submit that these conditions are "baked in". In other words, the rules-in-use reflect the influence of those conditions (Carter et al. 2015). The hypotheses discussed in this chapter reflect this idea. For example, if Top Management are strongly supportive of securing cyber assets, the rules-in-use will reflect their participation throughout the security governance model. Further, an organization that requires top management participation via formal rules indicates a stronger governance structure than an organization that has no designation of top management participation written or otherwise.

The presence of those rules, and their effects upon the actors as they make choices, will be reflected in the policy documents produced by this process. These expectations form the central hypothesis of this study: that a more formal, and thus more effective, cybersecurity governance structure should produce relatively more effective policy than an ad hoc, and less effective, governance structure.

The unit of analysis is the case, a university selected for this study. Much of the evidence used in this study focuses on policy documents, and more specifically, the statements that comprise those documents. I refer to these data as "units of observation". Units of observation refer to "entities at which data are collected"

(Babbie 2004, 95 cited in Basurto, et al. 2010). I aggregate these observations to identify configurations of statements that form patterns defining the structure of policy and policy making (governance) for each case.

The IAD tools provide the analyst a means for a robust, systematic analysis of these observations. The analysis provides details at a level of precision that is finer than the document level of analysis employed by studies such as the analysis of university policies discussed previously (Neil Francis Doherty, Anastasakis, and Fulford 2009).

That study identified document types (standards, guidelines, etc.) and policy areas (e.g. password protection) via review of the policy objectives noted in each document. The Institutional Grammar tool disaggregates components of institutions observed among policy statements within such documents. For example, the Attribute of a statement identifies the entity responsible for accomplishing the objective or goal (component is aIm) within a statement.

Before we get down to this level of analysis, it is important to tie structure back to the analysis of documents upon which the findings of prior research is based. The chapter begins with an effort to connect the prior efforts using document analysis to this study's use of statement analysis by suggesting how the conceptualization of policy structure is treated by both approaches. The next section proposes thoughts regarding how varying organizational conditions, particularly the concepts of Top Management Support and Collaboration, are manifested within those structures. Finally, I examine the relationship of essential elements of policy structure and the structure of governance.

3.1 Conceptualizing Policy and Governance Structures as Networks

Doherty, et al., conceptualized Policy Structure by asking three questions: 1) how many types (issues covered) of policy are available; 2) How many documents compose the information security policy; 3) how do the documents relate to each other vis-à-vis lower level standards and procedures (2009). Those structure types and the attributes of the documents described by Doherty are similar to terms found in social network analysis. One can create a scale from "no relationships" to "ad hoc" relationships (with few connections among the documents), to clusters of documents with inter-connecting references (cluster network) to a single large cluster (formal network) with relations among lower level documents (standards and procedures).

Security documentation must provide clear references to connect the various documents and the issue areas those documents address (Doherty, et al 2011 p. 205). The types of documentation identified by Doherty, et al, includes procedures, forms, guidelines, standards, and policy statements. Effective security relies upon clear references between these documents as well as some consistency in the naming of those documents (Doherty et al 2009). Analysis of policy structure is focused on the understanding of "the number of policies in use and how these relate to each other and to lower level standards and procedure" (Neil Francis Doherty, Anastasakis, and Fulford 2009, 451).

One can represent the connections between document types (standards, procedures … as Doherty labeled them) and policy issues as a network graph. Ideally, all types and issues will be interconnected as they are in the formal network shown in

Figure 3-1. The formality of the policy structure is dependent upon the resources invested to create and maintain that structure. As the structure grows more formal, the graph evolves, showing more connections at varying component levels.

The different document types are represented by the shapes on the graph. The different policy areas are shown as colors. So a well-constructed policy for an area will show vertical links between the procedures (solid diamonds) standards (open squares), policies (solid squares) and meta-policy (sphere). The interconnection of document types across areas is a horizontal connection as shown in both the Informal and Formal graphs. The criteria for each type of policy structure is found in Table 3-1.

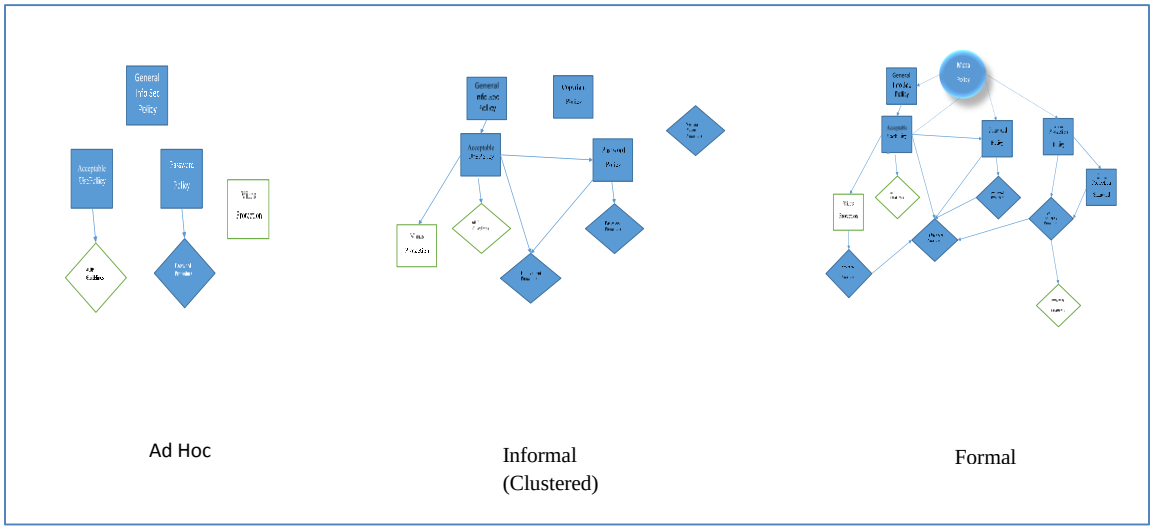

Figure 3-1 Sample Policy Structure Type
Legend: Sphere – Metapolicy, Solid Square – Policy, Square – Standard, Solid Diamond – Procedure, Diamond - Guideline

Table 3-1 Policy Structure Defined as Network Types

Policy Structure	Value	Description
None	0	Absence of general info sec policy, no links among policy documents
Ad Hoc (Loosely Coupled)	1	A general Information Security Policy, accompanied by a number of related policies and supplemented by specific guidelines and practice-related documents. Policy documents have little, if any, references to other existing policies
Informal (Cluster)	2	Policies and standards, supplemented by a number of related guidelines and procedures, with each guideline or procedure focused on one aspect of security mgt. The documents x-reference across types of security issues. . *A map of these policies demonstrates vertical links between policies, standards and procedures with few horizontal links connecting types of security issues. [emphasis mine].* A map of documents would present the horizontal links missing in the Ad Hoc structure.
Formal (Emergent)	3	A series of inter-related, cross-referenced policies (separate system, product, community, and corporate information security policies) –governed by a Meta Policy.

H1: The structure of a policy governance process will be reflected in the formality of the policy structure created by that process.

Intuitively, one expects that a formal policy structure is created by a similarly formal governance structure. Conceptually, a comparative measure of governance structure may be created by comparing the presence of Knapp processes used by an organization to the ideal Knapp model. We know from the review of literature that a dynamic, well-structured policy process increases the effectiveness of security policy (Baskerville and Dhillon 2008; Neil Francis Doherty, Anastasakis, and Fulford 2011; Moule and Giavara 1995; Baskerville and Siponen 2002). The Knapp processes of Risk Assessment, Development, Review, Retirement and Approval taken together compose the basic features of the *policy governance structure* for cyber security for each case. It is the combined outcomes of these processes that produce policy documents and practices to be implemented. The Knapp processes of Awareness, Implementation, Monitoring, and Enforcement comprise a process dimension of *policy operational structure*. The relationship between the presence and structure of individual Knapp processes, the governance structure, and policy structure is summarized in Table 3-2.

A crude test of relative "strength" of structure relies on the configuration of institutions in each Knapp defined process. A frequency analysis of observations coded for each Knapp process for each case provides measures of "relative strength" of processes. A "Weak" structure has fewer statements in a process than the average of all cases. A "Present" structure has average or above statements. "N"o presence is coded when no statements are present for the process.

3.1.1 Structural Components

The grammatical analysis of statements found in policy documents provide data to align those statements with the types of policy components identified by multiple researchers. The precision of analysis may improve as we move from documents to statements and identify these components.

Baskerville and Siponen (2002) suggest that emergent organizations require a meta-policy that governs the creation, implementation, and enforcement of security policies. Moule and Giavara (2009) define policies, standards, guidelines and procedures as components that comprise a framework employed to manage "guiding" information for an organization implementing a technology plan. Rees et al (2003) defines security policies as "... generally high-level, technology neutral, concern risks, set directions and procedures, and define penalties and countermeasures if the policy is transgressed". The authors distinguish the policy from "… implementation specific information" found in security standards, procedures and guidelines.

Table 3-2 Presence of Knapp Process per Structure type

IAD Framework	Knapp Governance Model		Structure		
Level of Analysis	**Action Situation**	**Description**	**Ad Hoc**	**Informal Network**	**Formal Network**
Collective	Approval	Actions required to approve policy; to operationalize the policy	W	W	P
Collective	Development	Activities include issue identification, definition of scope, research and analysis and stakeholder input	W	P	P
Collective	Retirement	Removal of policy from active service	N	W	P
Collective	Review	Management review of policy performance, alignment with business objectives, and effectiveness given other emerging technologies and security issues	N	W	P
Collective	Risk Assessment	Identification of organizational values, policies that may be compromised if certain behaviors are allowed to occur	N	W	P
Operational	Awareness and Training	Efforts to communicate to the campus community and to train them in the issues related to the policy in question	W	W	P
Operational	Enforcement	Judgment of whether a violation of policy occurred; application of sanctions	N	W	P
Operational	Implementation	Operational level application of the rules and norms contained within the policy document	W	P	P
Operational	Monitoring	Observation of policy compliance, audits of systems, use of automated tools to scan for behaviors not allowed	N	W	P
Legend: (P)resent; (W)eakly Present; (N)ot Present					

The configuration of policy components, as defined in table 3-3, represent increasingly specific sets of activities to support policy outputs and outcomes.

Table 3-3 Security Policy Components Defined

Policy Component	Literature	USG
Meta Policy	Establishes how info sec policies are created, implemented, enforced (Baskerville & Siponen 2002)	Not mentioned
Policy	Describes management's requirements at a high level, defining "what is required" not "how to do it".(Moule & Giavara) Defines importance of information assets to organization Defines management, employee responsibility to safeguard the resource Expresses concerns/objectives at "highest level of abstraction" (Baskerville and Siponen, 2002)	a concise document that outlines specific requirements, business rules or company stance that must be met. The policy is the organization's stance on an issue, program or system. It is a rule that everyone must meet.
Standard	Established rules or requirements that must be observed in the execution of procedures. (Baskerville and Siponen 2002) May provide specific security measures Often carry statement of sanction for non-compliance	a requirement that supports a policy Define minimum requirements designed to address certain risks Define specific requirements that ensure compliance with policies Outline implementation and enforcements plans Balance protection with productivity
Procedure	A series of specific instructions which must be followed in order to comply with prescribed policies and practices (Moule & Giavara)	Define specific requirements that ensure compliance with policies Provide a basis for verifying compliance through audits (USG lumps standards and procedures together as "standards")
Guideline	suggestion, approach or issue that the reader should keep in mind when performing a particular task or activity (Moule & Giavara)	a document that suggests a path or guidance on how to achieve or reach compliance with a policy.
Ancillary Policies	Not defined in the literature	Organizational policies not considered part of security framework – e.g. student handbook, faculty handbook, etc. but referenced for enforcement or credibility reasons – perhaps as external mandates

In practice, the University System of Georgia recommends the use of these components as part of its policy program governing the campus CIO's and CISO's[16]. The System's policy program uses defined categories of instructions that are similar to those identified in the research literature. The creation of Table 3-3 is a straightforward alignment of those definition and categories. There are two exceptions. The USG does not define procedures as a separate class of instructions, consolidating the definitions for procedures within the term "standards" in their documentation. Second, the concept of a metapolicy is not directly referenced. Nonetheless, the components identified by research is validated in practice by the USG documentation.

How may these components relate to observed features of governance structure? The existence of a meta-policy implies the presence of most, if not all, of the policy components. This statement is particularly true if the meta-policy is found in a formal document. The absence of a formal meta-policy suggests that components may be missing. The next set of hypotheses will explore this question.

A formal, or written meta-policy is the outcome of the investment of actors within an organization to publicly acknowledge how policies are to be developed, reviewed, retired, and implemented. A meta-policy indicates an emergent organization that provides structure to allow individuals and sub-units of an organization the latitude to adapt policy as needed. Standards, procedures, policies, and guidelines are provided within emergent organizations to assure that such adaptations are done with minimal

[16] University System of Georgia Information Security and ePrivacy – Policy and Compliance Management found at http://www.usg.edu/infosec/policy_and_compliance_management. Last Accessed 3 Aug 2012.

adverse effect on desired organizational outcomes. The existence of a meta-policy implies a culture that adopts and promotes best practices. In sum,

> **H2**: If an organization possesses a meta-policy then the likelihood that that organization observes most if not all of the processes identified in the Knapp model is greater than an organization without a meta-policy.

The presence of a nearly ideal Knapp model in an organization will correlate with an appropriate configuration of all policy components. However, as Baskerville and Siponen observed, meta-policies are not ubiquitous among organizations. The absence of a meta-policy suggests a governance structure is missing, or at best presents weak, governance processes. A deficient structure is defined as one that is missing a Knapp process or presents a weakly structured process (i.e. few formal rules/actors).

3.1.2 Policy Components and Formality of Structure

A meta-policy is not an approach that generates a "one size fits all" set of policies for an organization. A meta-policy, properly constructed, is a framework that governs policymaking in a manner that recognizes the need for organizational units to tailor policy to fit each unit's respective needs in the context of organizational goals, mission, and objectives. An important characteristics of an emergent organization is the reliance on decentralization of policy management (Baskerville and Siponen 2002, 340). Decentralization introduces opportunities for innovation and exploration of means to promote the ease of use of the policies to secure cyber assets (Baskerville and Siponen, 2002, 341). Many of the requirements of a formal meta-policy defined by Baskerville and Siponen to meet the needs of an emergent organization align with the processes

identified in the Knapp model and the components of policy identified in the literature. Therefore:

> **H3:** An effective formal governance structure presents a full complement of components and Knapp processes to be effective.

The hypotheses express the expectation that a more formal, and thus more effective, governance structure should produce relatively more effective policy than an ad hoc, and less effective, governance structure. The hypothesis presumes that anything less than a formal structure will present missing processes or components. As the governance structure moves from a formal to informal to ad hoc structure, the number of missing processes and components will increase. Missing components and processes are symptoms of an ineffective policy. For example, a policy without monitoring and enforcement cannot effectively contribute to desired outcomes. The hypotheses suggests a continuum that correlates to the increasing deficiencies in policy structure.

For example, I suggest that an informal structure has definitive statements defining activities within Approval, Development, Review, Risk Assessment, Implementation and Monitoring. The appropriate policy components, representing policies, standards, procedures and guidelines, are present. Retirement, Awareness, and Enforcement activities may not be strongly present, if at all. But, the essence of a learning cycle – which requires monitoring of behaviors, assessment of risks, and review of policy performance – is present. It is likely that required policy areas have varying mixes of components. A common Acceptable Use Policy (AUP) is likely to possess most

of the policy components, clearly assigning responsibility and procedures to management, staff, and casual users.

Policies created within an informal governance structure will present a more diverse set of policy components (e.g. standards, procedures, and guidelines) which improve the effectiveness of security efforts (Moule and Giavara 1995) than a policy structured in an ad hoc governance process. In addition to filling the "vertical" spaces of the policy component table, a map of policy documents will present a number of the components linked horizontally across policy areas revealing a cluster network structure. The horizontal links serve to reference procedures and guidelines that can be applied regardless of the policy area. Enforcement and judicial procedures to determine guilt and punishment are an example of processes that can be applied to most policy infractions. Improvements to the policy structure, as compared to ad hoc processes, may be related to strong leadership, an adopted design philosophy, or a strongly collaborative organizational culture.

An ad hoc policy structure may be the norm for many organizations (Baskerville and Siponen 2002). There is no formal meta-policy document available to define the process. The policy statements for the Knapp processes, if there are any to be identified, are likely to represent the guideline or ancillary components of policy. The process for approval may exist, but the positions within that process that are given the decision-making powers to approve, or not, are unlikely to be inclusive, or similar to, the organizational decision structure. Most likely, the CIO or CISO will unilaterally approve, or not approve, the policy. The statements identified with approval are likely to be

identified as standards and policy components. The other Knapp processes (M)aybe present, and will feature statements that tend to be more norm than rule, are not inclusive of the organizational membership, have relatively little information required to be presented for consideration, and little sanctions, or rewards, to incent the desired behavioral outcomes.

3.2 Organizational Conditions – Relationship with Governance Structure

The literature review finds two organizational conditions, Top Management Support (TMS) and Collaboration, as necessary for effective policy and policy management. Literature from research on higher education acknowledges the effects of autonomy as a cultural value that may frustrate changes of policy necessitated by the dynamic environment of cyber security. These conditions are recognized as organizational conditions by the research model. I hypothesize that these conditions will be observed in the structure and configuration of the policy statements observed as rules, norms and standards.

3.2.1 Top Management Support (TMS)

Board of Regents policy sets constitutional-level rules requiring a) the President of each college or university ensure that a cybersecurity program is in place; and, b) that the CIO for each BOR organization will create and maintain such a program. These requirements fall into the category of “Compulsory Boundary Rules”. If Top Management Support (TMS) for cybersecurity is low, then one expects that an organization will proceed with these two actors as the primary decision-makers. The

CIO is likely to informally charge his or her staff, a compulsory rule with an implied eligibility determined by position on the IT staff, with the responsibility of drafting policies. But, the final decision as to which policies to develop and how those policies are word will be made by the CIO and President. If TMS is high, then one expects to see representation for all campus sub-units.

Recall from chapter 2: "governance institutions are used by the organization to 'enable the selection of agents to act on its behalf in different decision contexts, thus affecting the actors and positions they hold within the focal action situation'" (McGinnis 2011b, 54). The influence of top management support is observed in the institutions that guide behavior (Purvis, Sambamurthy, and Zmud 2001). Top Management Support is measured by a proxy that identifies actors holding top positions given responsibility by the governance rules for tasks related to the development, review, and approval of policy. Attributes and conditions of Boundary rules define 'who' and 'when' may enter and exit the action situation.

Ostrom and Crawford classify boundary rules as three types (2005b, 194). Eligibility boundary rules determine who may hold a particular position. Entry boundary rules define the process by which actors may/must enter a position. Exit boundary rules define the process by which actors may/must leave a position. Ostrom and Crawford further classify boundary rules as first and second-order. First-order rules define eligibility of individuals to hold a position. Second-order rules classify those who are eligible to participate into "subsets of position-holders and non-holders" (2005b, 195). Open boundary rules enable an individual to opt in to holding a position. Invitation

rules require an invitation from positions of authorities inviting eligible members to accept a position. Compulsory rules deny an individual the choice to accept a position. Competitive rules require a competition to determine who may hold a position. Variation in conditions of entry, attributes, and deontic of the rules alter the structure of a situation by changing who participates in the process.

I suggest that the number of principals of the organization specified to participate by first order rules within the governance structure is a proxy for Top Management Support (TMS). The intention of a first-order rule is clear. If you occupy a position of leadership in an area critical to the success of information security, then you should participate in the governance of security policy. Requiring actors to participate may be seen as action on the part of top management to make security a priority of the organization.

> **H4a**: Governance structure will resemble the ideal Knapp model as the number of principals identified in 1st order boundary rules increase.

The IAD framework identifies one rule type, Boundary rules, that determine participation in decision-making arenas. Best practice and theory find that participation of Top Management is necessary to assure policy effectiveness. A compulsory boundary rule possesses a "Must" deontic versus a "May". Therefore:

> **H4b**: High TMS is likely accompanied by compulsory Boundary rules requiring the participation of a number of principals of the organization.

The literature describes a "default" configuration for the role of IT personnel as the primary driver of security policies. A process without meta-policy statements reflects this default condition.

H4c: If there are no compulsory boundary rules, then the likelihood that a techno-centric governance process increases. TMS will be "lower" than in organizations with compulsory boundary rules.

3.2.2 Collaboration

A solitary rule type does not define the structure of a situation by itself. If the TMS is low, then the choice rules (denoting who has the power to decide final outcomes) are likely simple and designate the CIO, most likely, as the primary decision-maker. If TMS is high, then the addition of other actors implies a more sophisticated choice-rule structure. Aggregation rules, those that determine how decisions are made, will reflect the likely condition that the CIO or CISO makes the final decision regarding policy content and structure without consulting stakeholders, which might require a consensus for approval.

Collaboration is essential to securing cyber space (Goodman and Lin 2007, 227). The literature confirms that institutional rules, and organizational context, are important factors in determining the effectiveness and likelihood of collaboration (Hardy and Koontz 2009). Effective policy, therefore, requires a governance structure that permits and encourages collaboration in the production of policy.

Among the goals found in the USG Information Technology Strategic Plan, is the implementation of a commons security management framework to ensure "trustworthy information sharing, analysis and collaboration" ("Information Technology Strategic Plan" 2010, 24). An important characteristic of collaborative governance is the inclusiveness of "all stakeholders who are affected by or care about the issue" (Chrislip and Larson (1994) as cited in Ansell and Gash 2008, 556). This characteristic suggests

that an Open Boundary Rule allowing any persons with an interest to opt in to the policy situation will be present.

Open Boundary Rules support collaboration and collaboration is consistent with an emergent policy structure.

> **H5a**: The presence of Open Boundary Rules setting the criteria for participation in making security policy reflects an organizational condition that values collaboration. An Ad Hoc structure will be the least likely to present Open Boundary rules. A Formal structure is likely to present Open Boundary Rules.

An Invitation boundary rule may be required to insure effective leadership participates in the process as the lack of effective leadership may decrease the likelihood of effective collaboration (Ansell and Gash 2008, 555).

> **H5b**: The absence of an invitation boundary rule specifying participation of university leadership will increase the likelihood of a governance structure that is largely ad hoc in nature.

Being present is necessary, but not sufficient, to assure collaboration. Aggregation rules specify who decides whether and which action may be taken (E. Ostrom and Basurto 2011, 323). Aggregation rules are most likely, and most necessary, when "choice rules assign multiple positions partial control over the same set of action variables" (E. Ostrom and Crawford 2005b, 202). Ansell and Gash (2008), citing Connick and Innes (2003) and Seidenfeld (2000), note that decision-making within collaborative governance is "consensus oriented." They conclude: "the goal of collaboration is typically to achieve some degree of consensus among stakeholders" (547).

Ostrom and Crawford identify three types of aggregation rules that define outcomes: non-symmetric, symmetric, and rules that define outcomes when agreement

cannot be reached (E. Ostrom and Crawford 2005b, 202). Non-symmetric rules provide actors with variable capacity to render a decision (2005b, 203). Non-symmetric rules may assign a subgroup with power to make decisions under certain conditions. Symmetric rules ensure that all participants possess similar power over outcomes. Such rules may state conditions of consensus or require unanimity before an action is taken. Studies of agreement rules have found that variation of just this part of a rules configuration can have great effects upon outcomes and illustrates the importance of examining rules configurations and not just single types of rules (2005, 205).

> **H5c**: The presence of symmetric Aggregation rules along with Open Boundary rules reflects existence of a collaborative culture and the governance structure is more likely to resemble a completed Knapp model.

Consensus depends upon trust among the actors. Trust is dependent upon reliable access to information. Information rules determine what participants know of an action situation (topic); from whom participants gain information (channels); how often participants are given information (frequency); how reliable the information may be (accuracy); and even the codes or languages used to communicate (language) (E. Ostrom and Crawford 2005b, 206–207). Various configurations of information rules may alter the power within an action situation and therefore the outcomes. For example, a study of occupational subcultures of IT employees found that dysfunction in communications among these groups can have negative effects on the organization (Guzman et al. 2004, 79). The absence of a process to exchange information across individual policy areas complicates and frustrates efforts to understand the policy and to implement the policy within the organization (Baskerville and Siponen, 2002, 341).

H5d: The presence of information rules requiring the exchange of information among actors indicates the existence of a collaborative culture and indicates a stronger governance structure when compared to cases without such rules.

3.2.3 Autonomy

Autonomy describes a key component of the culture of the university that dominates all levels of the organization from the individual faculty member to the systems and associations that govern public institutions of higher education (Christensen 2010). The strength of the desire for autonomy has influenced the governance structure common to most universities and colleges. The influence of autonomy contributes to an organizational structure that Cohen and March (1972) describe as a form of organized anarchy with a policy process best euphemized as akin to producing good eats from a "garbage can". To wit, Weick (1976) described higher education as many "loosely coupled systems." Each of these authors attempts to describe an organization of multiple sub-units that possess either autonomous or semi-autonomous governance authority with respect to the larger institution. Autonomy, therefore, makes change and innovation, even when driven by external mandates, slow at best, or inhibited, at worst (Bartell 2003) as these sub-units attempt to collaborate, to decide how and whether to act.

Intuitively, I expect that an organization with strong values regarding autonomy will exhibit a diffuse governance structure. In other words, the ability to make decisions regarding policy are distributed across and down the organizational structure. Scope rules define outcomes that must, must not, or may be affected by actions taken (Ostrom and Crawford 2005b, 208). Scope rules constrain the range of outcomes available

(Ostrom and Crawford 2005b, 208). A scope rule may be used to affect an outcome otherwise not attainable using choice rules. A specific example is given within the context of universities where the norms and rules governing academic freedom may make efforts to restrict how a professor teachers as suspect, but rules that encourage or incent specific outcomes, thus encouraging professors to choose a particular method, as permissible (Ostrom and Crawford 2005b, 209).

How does a governance structure that protects autonomy differ from an emergent organization that complies with enterprise policy objectives? In this case, a department, with strong autonomy, could choose to ignore a policy written by the CIO. The department is able to do so when monitoring and/or enforcement processes are not present. Autonomy is protected when the deontic for the policy statements is permissive (may) and not obligatory (must). Autonomy is protected when actors from the department are not obligated to participate in the development of policy and when those actors are not required to share information with others as to policy implementation, or methods used to meet policy objectives. Autonomy is less threatened in an ad hoc structure than an informal structure but is more likely managed in a formal governance structure as all the processes required to implement, and to manage tailoring and implementation at the department level, are available for managing unit level implementation.

> **H6**: If Scope rules limit actions of sub-units to modify policies, the governance structure is likely to resemble a Knapp model.

3.3 Elements of Policy Structure

The role of cyber security policy is to provide rules to govern individual behavior as that behavior affects the information and technology resources of their organizations (Whitman 2008). Information security policy defines the roles and responsibilities of the employees to safeguard the information and technology resources of their organizations (Bulgurcu, Cavusoglu, and Benbasat 2010). The composition of policy includes written policy documents consisting of many textual statements that regulate the behavior of an organization, its sub-units, individual employees, and policy makers (Weible and Carter 2015).

Most of the articles addressing policy content have been prescriptive in nature (Baskerville and Siponen 2002). From these prescriptions, a synthesis suggests four dimensions conceptualized as variables derived from policy content that affect the relative strength of policy effectiveness (Figure 3-2). The main working hypothesis of this study is that there is a correlation between elements of policy structure such as components, scope, tailoring, and form that correlate with structures within the Knapp governance processes.

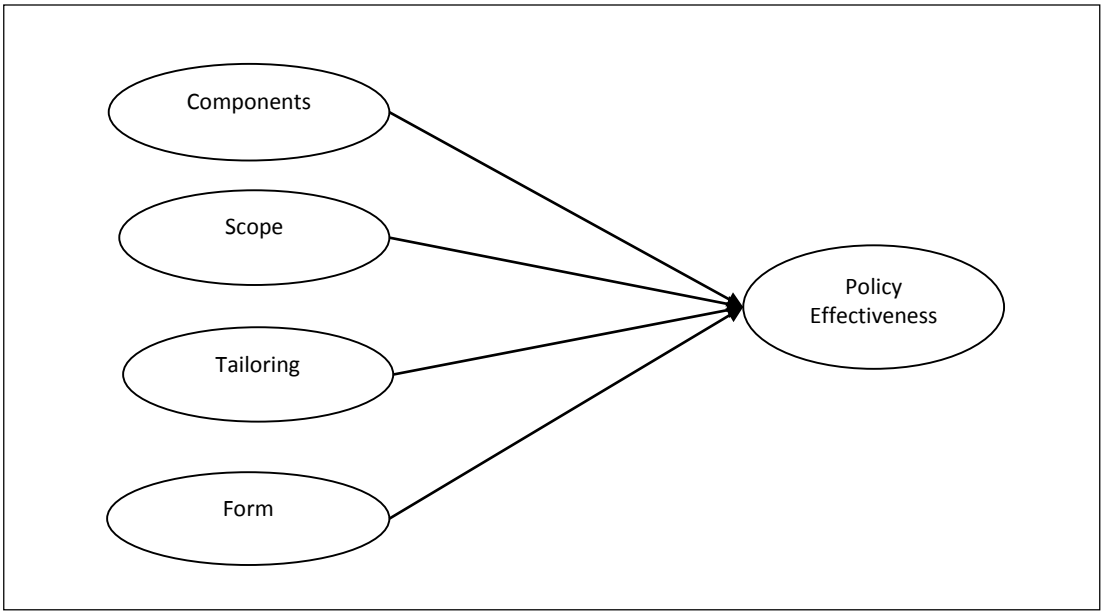

Figure 3-2 Elements of Policy Structure

The lack or relative weakness of these qualities may be termed as deficiencies in policy structure. Deficient policies may possess "inconsistent formats, inappropriate scope, incomplete structure and coverage of subjects, ambiguous wording, and weak coupling between risk and intent" (Knapp et al. 2009, 502). Such deficiencies in governance structure can be found in a weak or non-existent policy for policy development, review, or lack of feedback from key constituencies.

Security policies are ineffective, becoming "paper tigers" (Bjorck 2004), when the desired security behavior does not become part of the organizational norms (Backhouse and Dhillon 1996, 8), a condition related to weak or non-existent means to tailor a policy, or to make stakeholders aware of a policy. The lack of awareness of a new or revised policy will decrease the likelihood that the new norms will become part of the organizational culture. In the following section, I offer hypotheses concerning

relationships between the structural elements of policies and the structure of governance that created those policies.

3.3.1 Components

The presence of a nearly ideal Knapp model in an organization is likely to correlate with an appropriate configuration of all policy components. If the appropriate components are present in the governance structure, it is likely we will find a similar set of components in the policy structure. An informal or ad hoc governance structure will likely not present needed components of standards, procedures, and guidelines that help the organization to implement and manage a policy effectively.

> **H7**: As an organization's governance structure declines from Formal to Ad Hoc, then it is less likely to present a coherent set of standards, procedures, guidelines and policies appropriate for effective policy.

3.3.2 Scope

The objectives, issues, and topics of policy statements, as explicitly stated, define policy scope (Neil Francis Doherty, Anastasakis, and Fulford 2011, 203). Scope, says Hong, et al., refers to the coverage of relevant security issues which have been identified by multiple standards (see ISO 17799, COBIT, and others noted by Hong, et al (2006) and Hone and Eloff (2002)). As the comprehensiveness (coverage) of content increases, so does policy effectiveness (Hong et al. 2006, 113). The baseline security policy document structure given the USG requirements is seen in Table 3-4.

Table 3-4 USG Baseline Document Structure

Coverage Required	Policy Objective
USG Info Sec Policy Section 11 (2011)	Requires all institutions to maintain an IS infrastructure and program to ensure confidentiality, availability, integrity of information assets
USG Password Authentication Policy	It is the responsibility of every Institution and the University System Office to implement authentication mechanisms such as passwords to access sensitive data and the responsibility of the user to appropriately select and protect their passwords.
USG Appropriate Use Policy	The USG expects all institutions and their users to use IT resources in a responsible manner, respecting the public trust through which these resources have been provided, the rights and privacy of others, the integrity of facilities and controls, state and Federal laws, and USG policies and standards.
USG Risk Management Policy	University System of Georgia (USG) Institutions must ensure the confidentiality, integrity and availability of information and information systems resources and assets by protecting them from unauthorized access, modification, destruction, or disclosure and ensure the physical security of IT resources and assets.
USG Data Handling and Storage Standard	This policy is intended to ensure that the information is uniformly used and disclosed in accordance with all USG policies and applicable state and federal laws.
USG Computer Security Incident Management Policy	This policy establishes the requirement for each University System of Georgia (USG) institution and the University System Office (USO) to establish an internal capability for handling computer security incidents.
USG - HIPAA Privacy and Security Policy	To meet the requirements of the HIPAA Privacy and Security Rules, the University System of Georgia, it's institutions; hospitals, GPLS and benefit plans will develop policies, which govern the use and disclosure of PHI.
USG Continuity of Operations Plan	This policy shall establish a requirement to develop a formal program to develop, maintain, and evaluate plans to appropriately respond to a wide range of contingencies and disasters that may occur at all of the USG institutions, System Office and Georgia Public Library Service.
Use of Cryptography	This policy establishes the requirement to use cryptographic controls on University System Office (USO) and University System of Georgia (USG) Institution information systems as necessary.
Security and Awareness Program	The USG's employees (full/part-time employees and contractors) shall be made aware of their basic information security responsibilities through an awareness program.
Electronic Data Disposal	All computer systems, electronic devices and electronic media must be properly cleaned of sensitive data and software before being transferred outside of the University System or GPLS, either as surplus property or as trash.
Copyright Violation Guidelines	The purpose of this guideline is to establish acceptable practices that support the policy as it applies to copyright violations.

A study identified three conditions: environmental uncertainty, competitive advantage, and resource availability, along with three organizational conditions: top management support, IT capability, and culture; as conditions that affect managers' perspectives of security requirements and the benefit of implementing those requirements (Hsu, Lee, and Straub 2012, 920). In other words, these conditions

affected the Information Rules and the Payoff rules that regulate the decisions made related to policy. Top Management Support reflects these perspectives. Therefore,

> **H8**: The likelihood of coverage of USG issues will correlate with the relative strength of top management support for securing cyber assets

3.3.3 Tailoring (Fit)

Karyda, et al (2005) describes the policy process as one of inputs, activities, and outputs embedded in social processes unique to the organization. If cyber security policy is to be effective, one must align security policy strategy, structure, goals and norms with existing organizational norms, processes and structures (Bohme and Kataria 2006). The content and structure of cyber security policies should accommodate the unique needs of an organization if desired outcomes are likely to be realized (Drevin, Kruger, and Steyn 2007). When structuring policy to improve situational awareness of cyber sec issues at the individual level, factors such as "conscientiousness, cultural assumptions and beliefs, social conditions that affect staff behavior, and attitude towards work " must be accommodated in the design (Eeten and Bauer 2009; Eeten et al. 2007; Gurpreet Dhillon and Torkzadeh 2006).

In sum, the "devil is in the details". Do the various policy statements that constitute Acceptable Use policies reflect differences in the users, the context, and the structure of an organization? Most prior research examines fit in concert with organizational mission and objectives. If these policies are not tailored to fit the organization, then their effectiveness is greatly reduced. Fitting a policy to an organization can be as simple as: referencing existing enforcement processes (e.g.

Faculty discipline policies, Student Judiciary proceedings); assigning responsibility to individual departments for monitoring; or assigning responsibility to various positions to implement the policy. Using the IAD tools, I will look for Attributes and oBjects containing references to organizational specific actors and ancillary documents (e.g. Faculty Handbook).

The organizational conditions requisite to encourage tailoring include strong TMS for security compliance and a culture that values collaboration so that language and structure will reflect a consensus of those affected. The absence of organizational specific references indicates a lack of tailoring of policy statements consistent with organizational context (Kotulic and Clark 2004).

> **H9**: Acceptable Use Policies will vary in "fit" as the governance structure varies. A Formal structure will provide greater evidence of fit, measured in terms of specific assignments and positions referencing that particular organization.

In order to measure fit, I use the rules typology developed within the IAD framework (E. Ostrom and Crawford 2005b; Basurto et al. 2010a; E. Ostrom and Basurto 2011); the definition of coverage areas (Table 3-5) assigned to Acceptable Use Policies (Neil Francis Doherty, Anastasakis, and Fulford 2011); and the components of institutional statements identified by the Institutional Grammar Tool (Crawford and Ostrom 1995). Analysis focuses on observations identified as part of Acceptable Use Policies (AUP) and assigned to operational level action situations such as Awareness, Implementation, Monitoring and Enforcement. The Implementation observations are then categorized as to the issue by criteria found in Table 3-5. The premise of the fit hypothesis is that a more formal governance structure will be supported by strong TMS

and a collaborative culture. Therefore, the positions identified via analysis of Attributes and oBjects will be more likely to be organizationally specific and will represent the organizational structure. The Conditions of the statement will also more likely reference the organization and its structure. And, the aIms, the goals or objectives of statements, will reference objectives specific to the organization.

Table 3-5 Coverage Areas – AUP
Source Doherty, et al, 2011, 204

AUP Policy Coverage Areas	
Issue	**Definition**
Access Management	Covers issues such as who is authorized to use systems and corporate information; username and password management regulations and good practice guidelines
Acceptable Behavior	covers permitted user activities, such as work-related use of the systems and information, and internet usage in particular.
Unacceptable behavior	Covers prohibited user activities, such as hacking, downloading illegal material, accessing illegal websites, dissemination of illegal or offensive material, sending bulk emails, harassment of other users, violating privacy of others users, dissemination of viruses, use of systems and/or corporate information commercial purposes, personal usage of systems and/or corporate information
License Compliance	Rules and regulations about software downloading, sharing and usage
Roles and Responsibilities	Explanation of the specific roles and responsibilities of users, system administrators, and so on
User Monitoring	Explanation of approach to monitoring user activities
Sanctions for policy violations	explanation of actions that will be taken in the event of a user breaching the acceptable use policy
Policy management	Details of responsibilities and procedures for policy management and maintenance

3.3.4 Form

Form is a dimension which includes the elements of clarity (is intent understandable) and brevity. How well a policy is written determine the effectiveness of the policy (Goel and Chengalur-Smith 2010). If effectiveness of security policy is dependent upon the individual and their behavior (Lane 1985 as cited in Backhouse and Dhillon 1996) then users must be able to identify and understand what is expected of

them as they use and manage cyber assets (Höne and Eloff 2002b). Therefore, policy should be written in a manner that focuses on the user (Höne and Eloff 2002a).

Goel and Smith identify clarity and brevity as two dimensions of form that relate to policy effectiveness (2010). In their literature review, Goel and Smith note that research evaluating the effectiveness of privacy policies found that most policies were incomprehensible to the general population (Sheehan, 2005; Anton et al., 2007 as cited in Goel and Smith 2010 283). Concepts such as clarity and brevity of policy predict the likelihood that users will understand the policies (p. 283). Goel and Smith operationalize clarity by grading policy statements using the Flesch Reading Ease Score (FRES) and Flesch-Kincaid Grade Level (FGL). The researchers operationalize brevity as a function of the total number of non-stop words (ex: in, and, the) divided by the number of unique words.

> **H10:** As the governance structure of a university becomes more formal, then the likelihood increases that clarity of the policy is more appropriate to the comprehension skills of the university's student population.

3.4 Summary

The research model and the hypotheses address the need identified by Orlikowski and Barley (2001, 153) to: "understand how institutions influence the design, use, and consequences of technologies, either within or across organizations". The hypotheses (Table 3-6) explore different facets of the research question, "How does policy structure relate to differences in policy governance?"

The first section of this chapter connected prior research using document analysis to this study's use of statement analysis by suggesting how the

conceptualization of policy structure is treated by both approaches. The next section explained how varying organizational conditions, particularly the concepts of Top Management Support and Collaboration, are expected to be manifested by the various types of rules within those structures. Finally, I discussed several hypotheses describing the relationship of essential elements of policy structure and the structure of governance.

Table 3-6 Study Hypotheses

Hypothesis	Component Tested
H1: The structure of a policy governance process will be reflected in the formality of the policy structure created by that process.	Governance Structure
H2: If an organization possesses a meta-policy then the likelihood that that organization observes most if not all of the processes identified in the Knapp model is greater than an organization without a meta-policy	Governance Structure
H3: An effective formal governance structure presents a full complement of components and Knapp processes to be effective.	Governance Structure -
H4a: Governance structure will resemble the ideal Knapp model as the number of principals identified in 1st order boundary rules increase	TMS
H4b: High TMS is likely accompanied by compulsory Boundary rules requiring the participation of a number of principals of the organization	TMS
H4c: If there are no compulsory boundary rules, then the likelihood that a techno-centric governance process increases. TMS will be "lower" than in organizations with compulsory boundary rules.	TMS
H5a: The presence of Open Boundary Rules setting the criteria for participation in making security policy reflects an organizational condition that values collaboration.	Collaboration
H5b: The absence of an invitation boundary rule specifying participation of university leadership will increase the likelihood of a governance structure that is largely ad hoc in nature.	Collaboration
H5c: The presence of symmetric Aggregation rules along with Open Boundary rules reflects existence of a collaborative culture and the governance structure is more likely to resemble a completed Knapp model.	Collaboration
H5d: The presence of information rules requiring the exchange of information among actors indicates the existence of a collaborative culture and indicates a stronger governance structure when compared to cases without such rules.	Collaboration
H6: If Scope rules limit actions of sub-units to modify policies, the governance structure is likely to resemble a Knapp model.	Autonomy
H7: As an organization's governance structure declines from Formal to Ad Hoc, then it is less likely to present a coherent set of standards, procedures, guidelines and policies appropriate for effective policy.	Policy Structure - Components
H8: The likelihood of coverage of USG issues will correlate with the relative strength of top management support for securing cyber assets	Policy Structure - Scope
H9: Acceptable Use Policies will vary in "fit" as the governance structure varies. A Formal structure will provide greater evidence of fit, measured in terms of specific assignments and positions referencing that particular organization	Policy Structure - Fit
H10: As the governance structure of a university becomes more formal, then the likelihood increases that clarity of the policy is more appropriate to the comprehension skills of the university's student population.	Policy Structure - Form

Chapter 4– Research Design

This chapter discusses the research design, case selection, data collection and data analysis under taken to answer the research question. A review of the logic model provides a visual map to help the reader see the relationship between the design and the research objectives. The research design employs a non-experimental multiple-case study. The case is the unit of analysis and the cases selected are four research universities. I walk through the case selection logic and discuss the data to be collected and the process employed to manage the collection. Much of the data collected must be broken down into statements so that both governance and policy structure may be understood. These statements are classified as units of observation that are aggregated to understand behaviors of the individual cases. The Data analysis procedures describe the methods for examining documents and interviews identifying institutional statements as units of observation. Procedures for interpreting the data are discussed also. The chapter concludes with a discussion on limitations of the design.

4.1 Review of Logic Model

The research design must facilitate the objectives of my research:

- Determine how does the structure of cybersecurity policy relates to differences in structure of policy governance of universities and colleges;
- Understand the relationships between policy processes (governance) and the outcomes (policy content, form, structure, effectiveness);
- Demonstrate utility of IAD framework and tools to discover governance structure, policy structure, and to analyze differences;

- Provide pragmatic suggestions for practitioners to create more effective policy to secure university cyber space.

The logic model I employ is derived from research agendas found in the fields of information security, organization theory, and institutional design. The theoretical frame serves as a foundation for the design (Figure 4-1). Information security research finds that effective security is a function of effective policy and policy management. Policy and management are regulated by the policy governance structure of the organization. The frame suggests that the key to creating effective policy is found within the governance of the policy process.

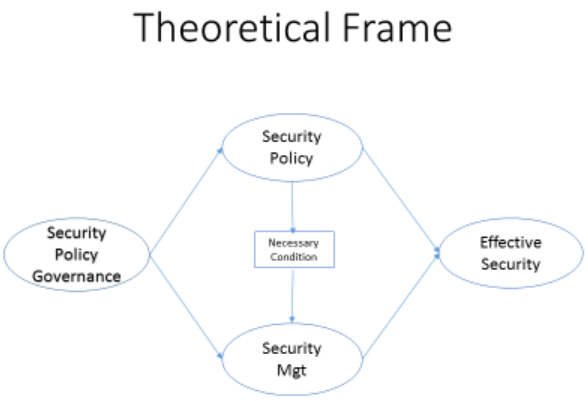

Figure 4-1 Theoretical Frame

Chapter 2 provides the background for selecting the IAD framework to create the basic research model (Figure 4-2). The model shows three levels of action that lead to security outcomes. My research objectives require an understanding of all three – the constitutional level as defined by the Board of Regents and legislative bodies; the governance level defined by each organization's processes to create and manage policy;

and the operational level where policy is implemented. The model acknowledges the influence of both organizational and external factors.

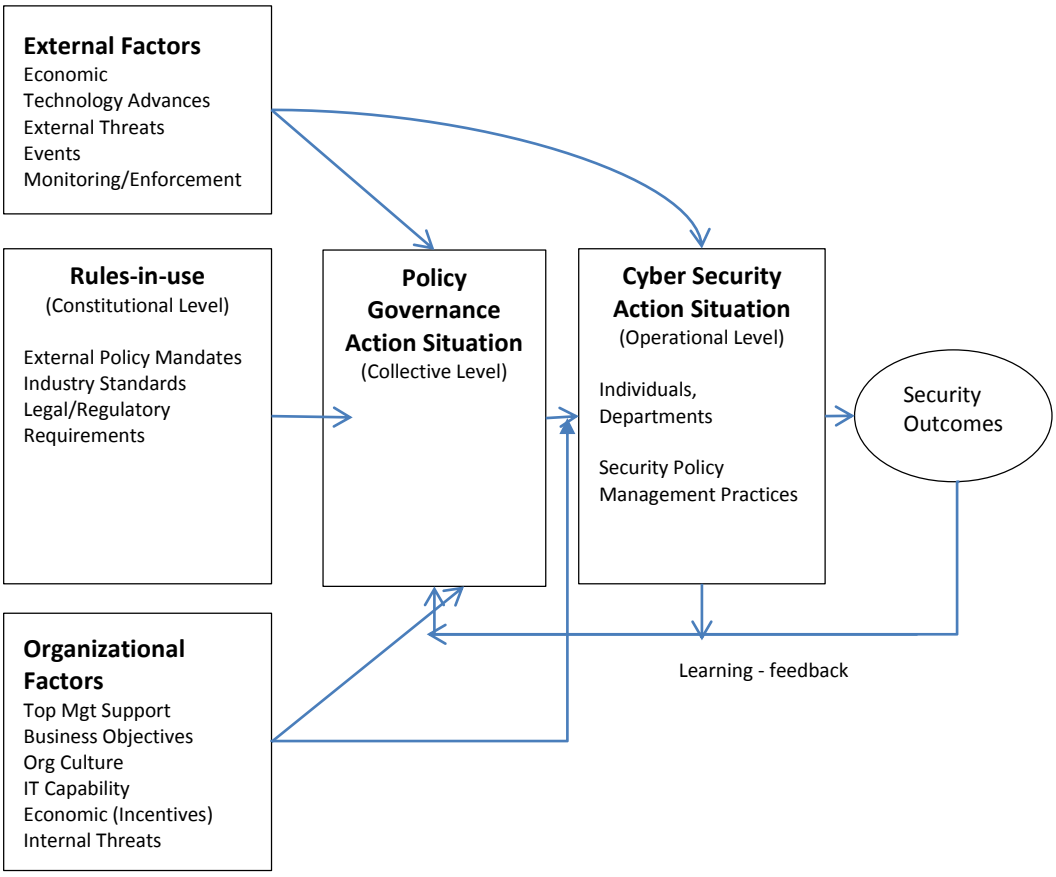

Figure 4-2 Research Framework Adapted from IAD

The Knapp model is a map of processes and factors that are necessary to create an effective security governance structure (Figure 4-3). The map is created from research that combined relevant findings of theoretical research with data captured from practitioners of cyber security.

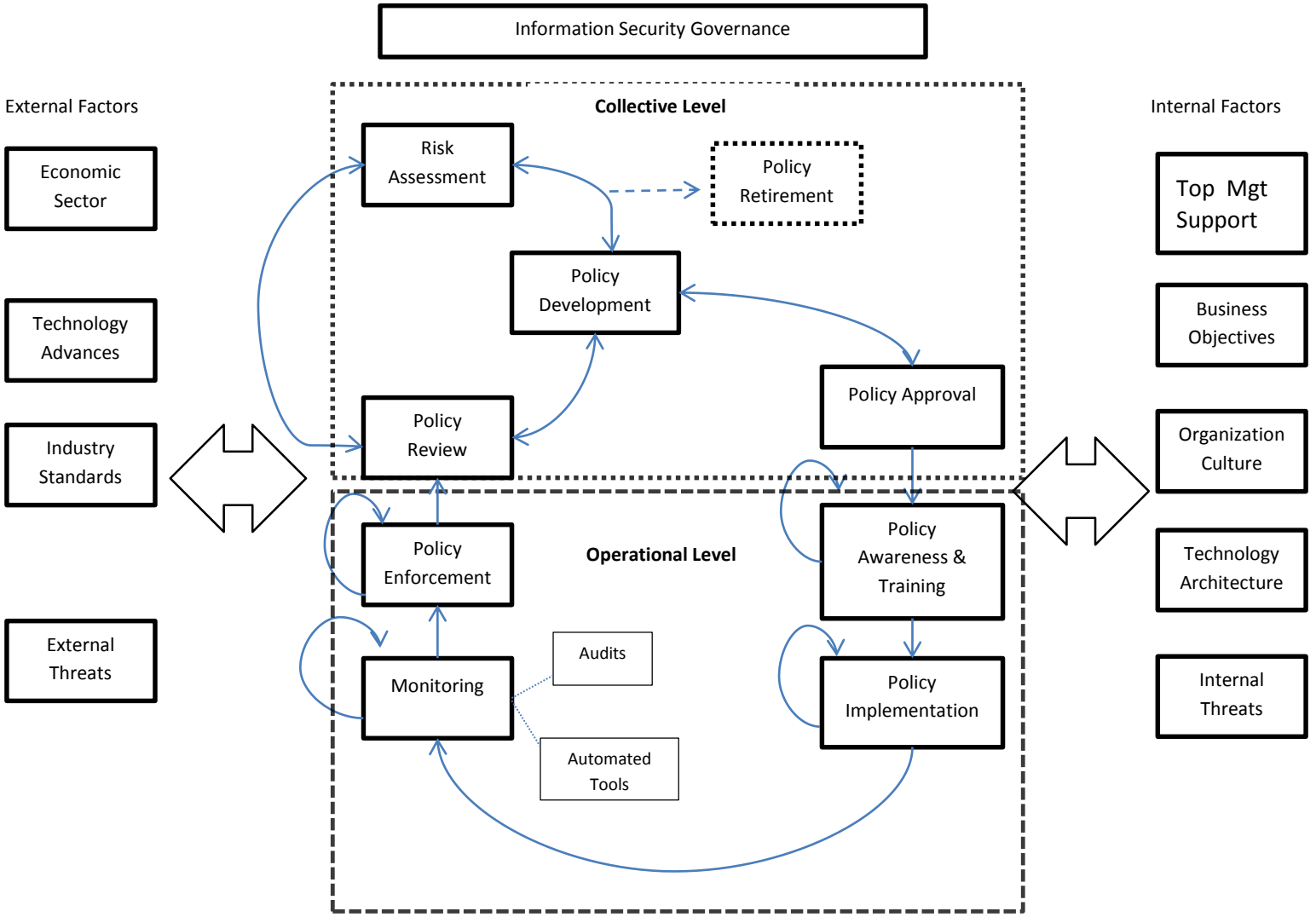

Figure 4-3 High-level Logic Model – Integrating Knapp with IAD

Each of the processes within the model represents an action situation where actors work within the procedures of each organization to create defined outcomes such as assessments of risk, new or revised policies, approvals, training, etc. Those situations are mapped to either the collective or operational level of analysis as defined by the IAD framework.

The framework provides a logic model to analyze the structure of an action situation (Figure 4-4). The structure of each of those action situations is defined by the actors and institutions employed by each case to create the outcome. The analyst can nest the structures of Knapp situations to define the structure in policy governance among organizations and, also, identify differences or variations of policy governance structure across the cases. The same approach can be employed to analyze, nest, and discern the structures, and variations among structures, of the operational level implementation of policies.

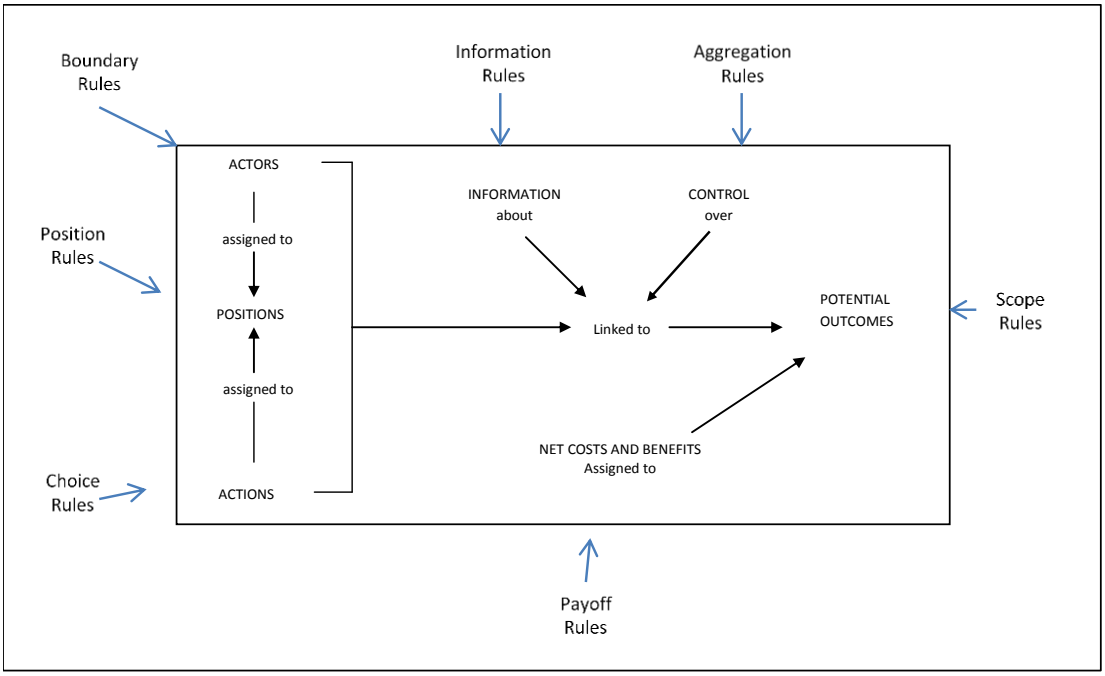

Figure 4-4 Analysis of Action Situation Structure

An institutional grammar categorizes the institutional statements by the structural elements found within an action situation (E. Ostrom and Crawford 2005b). The configuration of such elements suggests a method similar to genotyping can be used to trace structure back to higher level (i.e. organizational) traits and institutions (E. Ostrom and Basurto 2011).

The logic model provides a means of identifying the structure of the action situations; nesting those situations to analyze the structure of governance and operations; and to connect theoretical and pragmatic concepts from relevant fields of research. The research design will explain how I exercise the model to compare the structure policy governance and the structure of cybersecurity policy among the selected cases.

4.2 Research Design – Multiple Case Study

A research design represents the plan for connecting the data and the analysis of that data to the research question (Yin 2009). The research design designates the means to gather data, test hypotheses and present results (Hoover and Donovan 2007). In addition, the design offers acknowledgements of, and controls for, study limitations and biases known to the investigator. The research design for this study is a non-experimental, multiple-case study. A case study method is optimal when a "'how' or 'why' question is being asked about a contemporary set of events over which the investigator has little or no control" (Yin 2009, 13).

The research question asks "how does policy structure relate to differences in policy governance" in an attempt to explain why cyber security policy varied among

University System of Georgia campuses. The case study method has been used to test, extend, and generate theory (K. M. Eisenhardt 1989; K. M. Eisenhardt 1991; Miles and Huberman 1994; Yin 2003; Yin 2009). Case studies are commonly used for research of information security (Bakari, Tarimo, Yngstrom, Magnusson, & Kowalski, 2007; Bakari et al., 2007; Flechais & Sasse, 2009; Hassebroek, 2007; Hu, Hart, & Cooke, 2007; Iachello & Abowd, 2008) and is an appropriate approach to research where context is an important factor (K. M. Eisenhardt 1989). Case study designs are appropriate for the study of phenomenon involving information technology given the complex interactions among humans, organizations and technology (Dubé and Paré 2003). The approach forces a strategy of reliance on data convergence (e.g. triangulation) that benefits from prior theory to guide data collection and analysis (Yin 2009, 18).

Multiple cases permit the analyst an opportunity to "strengthen the precision, validity and stability of the findings" (Miles and Huberman 1994, 24). Multiple cases are "… discrete experiments that serve as replications, contrasts and extensions to the emerging theory" (EISENHARDT & GRAEBNER, 2007 citing Yin 1994, p. 25).

A replication logic design is not uncommon for multiple case studies (Yin 2009). Replication logic is comparable to experimental research designs (K. M. Eisenhardt 1989, 537). Literal replication involves study of cases thought to produce similar results. Prior research suggests that organizations of similar size, mission, and culture that demonstrate similar levels of top management support should adopt similar governance and policy solutions for securing cyber space. Theoretical replication involves studying cases predicted to yield contrasting results. Cyber security research also suggests that

organizations with different cultures and varying degrees of top management support will approach the problem of cyber security differently. Selecting groups of cases using both literal and theoretical replication logic can provide a richer explanation of the phenomenon under study by providing the analyst with rich data to observe contrasting effects of the same variables in different contexts (Yin, 2009 pp. 54-46).

4.3 Case selection

Resource constraints make sampling a pragmatic strategy of many studies, including this one (Dubé and Paré 2003, 609). An analyst must construct the sampling frame for a multiple-case study carefully using the research questions and model (i.e. conceptual framework) as a guide.

The research model contains a number of concepts, such as business objectives, culture, and internal threats that theory regards as antecedents to policy outcomes. Context also includes the actors, the organization, the culture and interactions among those concepts (Fendt and Sachs 2008). Context is important to understand the outcomes of decisions made within the action arena (E. Ostrom and Hess 2007). Holistic research efforts are characteristic of case studies and "suit well our need to understand the complex and ubiquitous interactions among organizations, technology, and people (Dubé and Paré 2003)". The contextual data encompasses the material conditions of each organization, the culture and structure of each organization that defines the community under observation, along with the institutions (rules, norms and standards) used to govern the individual members and processes of the organization.

4.3.1 Case Selection Criteria

A study of college administration found that as colleges and universities decrease in size, the likelihood that an administration would be bureaucratic (formal, centralized power) increased (Blau 1994). Research also suggests colleges and professional schools at research universities are more likely to demonstrate independence" from the central office (Blau 1994, 270). This study employs three basic criteria to choose individual units of the USG as cases: the Carnegie Classification, size[17], and rate of compliance with USG requirements.

The Carnegie Classification framework classifies organizations of higher education into categories that control for institutional differences[18]. Using the Carnegie Classification provides researchers with a means of categorizing cases to control for "extraneous variation and … defines the limits for generalizing the findings" (K. M.

[17] measured by the number of students registered for spring semester 2012 taken from the Spring 2012 Semester Enrollment Rpt - USG http://www.usg.edu/research/documents/enrollment_reports/spr2012.pdf last accessed 1 June 2012. Size, as defined here, is more precise than the size defined by Carnegie, allowing differentiation among USG units within basic Carnegie Classes such as AA, BA, and MA.

[18] Derived from empirical data on colleges and universities, the Carnegie Classification was originally published in 1973, and subsequently updated in 1976, 1987, 1994, 2000, 2005, and 2010 to reflect changes among colleges and universities. This framework has been widely used in the study of higher education, both as a way to represent and control for institutional differences, and also in the design of research studies to ensure adequate representation of sampled institutions, students, or faculty.
To ensure continuity of the classification framework and to allow comparison across years, the 2010 Classification update retains the same structure of six parallel classifications, initially adopted in 2005. They are as follows: Basic Classification (the traditional Carnegie Classification Framework), Undergraduate and Graduate Instructional Program classifications, Enrollment Profile and Undergraduate Profile classifications, and Size & Setting classification. These classifications provide different lenses through which to view U.S. colleges and universities, offering researchers greater analytic flexibility. These classifications were updated using the most recent national data available as of 2010, and collectively they depict the most current landscape of U.S. colleges and universities. (as found at http://classifications.carnegiefoundation.org/ last accessed 1 June 2012)
The methodology for assignment of classifications is found at http://classifications.carnegiefoundation.org/methodology/basic.php (last accessed 1 Jun 2012)

Eisenhardt 1989, 537) and allows for generalization of results to other organizations of higher education.

Employing the highest Carnegie category level, USG units are grouped into 4 areas – AA, BA, MA, and RU. As the categories shift from AA towards PhD granting universities, the mission, size, and complexity of the organization changes significantly. Literal replication supports selection of cases within the same Carnegie class. Within a class, I expect to find less different governance structures and policies than when comparing USG units across Carnegie classes as the factors describing context will be noticeably different.

Size is "one of the main differentiating structural factors among institutions" and is one of the more important elements determining structure as discussed within organization theory (Kezar 2006, 92). Structure, as we learned in chapter 2, determines how an organization governs itself. We expect processes to vary as organizational structure varies (Kezar 2006).

Compliance, the final selection factor, is measured by identifying the policies published by each USG unit and aligning the policy areas with those defined by USG requirements. Literal replication logic suggests an examination of units with similar compliance rates given similar missions should yield similar results. Theoretical replication logic suggests that compliance is related to size (i.e. as size grows so do fungible resources).

4.3.2 Case Selection: Data collected

Data collection for determining the sample population focused on summary case data (Appendix A) and an inventory of documents describing the information security policies for each unit of the USG (Appendix B). If not available on the web, documents were located by requesting them from the CIO's office of the USG unit. Protocols developed by Doherty et al, (2009; 2004; 2011) were adapted to create inventories of the policies by Policy Type and Coverage Area. In addition, the identification of type and coverage area provided data to suggest the policy document met USG required policy coverage. Every policy document found on a USG unit site received a unique id number, serialized, to serve as a reference throughout the database.

4.3.3 Cases Selected

The Board of Regents of the University System of Georgia has directed the USG CISO to:

> *… maintain information security implementation guidelines that the USO, all USG institutions, and the GPLS should consider in the development of their individualized information security plans.* Board of Regents Policy 11.3.2[19]

I compared the policies for each USG unit to the USG guidelines to determine compliance. A summary of compliance to those requirements is shown in Table 4-1.

[19] Found at http://www.usg.edu/policymanual/section11/policy/C430/#p11.3.1_general_policy last accessed 5 June 2012

Table 4-1 USG Units Policy Compliance

USG Policy Requirement	# Compliant	%	AA (n=12)	% AA	BA (n=4)	% BA	MA (n=11)	% MA	RU (n=5)	% RU
USG Info Sec Policy Section 11 (2011)	26	81%	8	67%	3	75%	10	91%	5	100%
USG Password Authentication Policy	21	66%	4	33%	3	75%	9	82%	5	100%
USG Appropriate Use Policy	32	100%	12	100%	4	100%	11	100%	5	100%
USG Risk Management Policy	11	34%	2	17%	1	25%	4	36%	4	80%
USG Data Handling and Storage Standard	23	72%	8	67%	3	75%	7	64%	5	100%
USG Computer Security Incident Management Policy	13	41%	4	33%	3	75%	3	27%	3	60%
Web Privacy Policy	14	44%	5	42%	1	25%	5	45%	3	60%
USG - HIPAA Privacy and Security Policy	4	13%	1	8%	0	0%	0	0%	3	60%
USG Continuity of Operations Plan	5	16%	1	8%	2	50%	1	9%	1	20%
Use of Cryptography	4	13%	2	17%	1	25%	1	9%	0	0%
Security and Awareness Program	4	13%	2	17%	1	25%	1	9%	0	0%
Electronic Data Disposal	10	31%	2	17%	2	50%	4	36%	2	40%
Copyright Violation Guidelines	14	44%	3	25%	4	100%	4	36%	3	60%

Legend: AA – Associate Degree schools; BA – Bachelors; MA – Masters and some doctoral programs; RU – Research University

The descriptive statistics (Table 4-2) for provides a quick picture of the variation in regards to population and policy compliance for each sector (BA to RU).

Table 4-2 Descriptive Statistics for USG Units

Sector	n	Avg Pop	Stdev	Avg # Policies	Stdev
AS	12	5450	6070	4.5	2.4
BA	4	5546	1513	7.6	3.1
MA	11	8411	5302	5.4	2.3
RU	5	21067	10799	7.8	0.4

An examination of four of the Research Universities as a complete group[20] provides an opportunity to examine more established units with significant outside resources (research grants, private grants, etc.) that also demonstrate significantly different business objectives in their mission statements (Table 4-3). The rate of compliance is the same for each of the four but the variation of size is a strong indicator of structural differences, and provides opportunity to examine more closely the effect of the different governance structures on policy structure.

Table 4-3 Selected Cases

Institution	Carnegie Class	Compliance USG Requirements	Population (Spr 2012)
University of GA (UGA)	DR	8/13	33367
Georgia State University (GSU)	DR	8/13	30606
Georgia Tech (GT)	DR	8/13	19431
Georgia Southern (GaSou)	DR	7/13	19150

4.4 Data Collection

The study used three primary methods of data collection. First, policy documents were located on USG unit web sites and downloaded to a local drive. Second, a survey of individuals accountable for managing cyber security policy for each unit provided information regarding the internal influences of the cyber security action situation. Third, interviews provided data regarding policy processes, structures, and rules that

[20] Georgia Health Sciences University was merged with Augusta State University and renamed Georgia Regents University during the time this study was conducted. Given the dynamics of the merger and the special nature of the school (a medical college), the author felt the unit was not well-suited for comparative analysis.

governed those processes. A triangulation of data collected by all three methods assisted in validating and clarifying the findings within the research model.

4.4.1 Case Summary Data

Descriptive data for each case was collected from three sources. The USG provided data regarding mission, enrollment, and the url for the campus web site and campus information security pages. Information regarding the current staffing for the positions of Chief Information Officer and Chief Information Security Officer was taken from the respective campus pages. Carnegie classifications were obtained from the Carnegie Institute web pages. The data dictionary for the case summary tables is found in Appendix D.

4.4.2 Documents

Documents were collected from each case. Most documents were obtained from the case websites. On occasion, the case contact supplied documents that could not be found otherwise. Interviews provided information as to the source of the policy development methodologies employed by each case. Those documents were sought from the appropriate standards organizations. Each document was processed according to the document protocol (Appendix C). Meta-Data for each document was collected as found in the Document Summary (Appendix E).

4.4.3 Surveys

The golden rule for constructing survey questions is: “Ask what you want to know, not something else” (Bradburn 2004, 3). A survey instrument from a prior study

(Knapp et al study (2007)) that identified the internal factors influencing the CSP action situation for each USG unit was adapted for the context of this study (Appendix F). A small sample of potential respondents (n=6) responded to the instrument. I interviewed the respondents (also testing questions for semi-structure interviews) to learn which survey questions were ambiguous or were unlikely to be answered[21].

I chose software manufactured by Qualtrics to manage the survey instrument. I invited respondents by email to answer survey questions online. Respondents clicked on a link generated by Qualtrics and inserted into the mail message. Follow-up emails were generated to non-respondents a maximum of three times.

The survey was sent to all IT professionals for each USG unit selected for study. The sampling strategy is valid for the following reasons. First, surveying only IT professionals is consistent with the population chosen by the Knapp study upon which the research model of this study rests. Second, technical solutions for security policy is the dominant strategy across all sectors (Gurpreet Dhillon and Backhouse 2001; M. Siponen, Pahnila, and Mahmood 2010; Mikko Siponen and Iivari 2006), including higher education (Baskerville and Siponen 2002; Bulgurcu, Cavusoglu, and Benbasat 2010). Third, the level of analysis for this study is the collective action level. The actors at the collective action level that develop and implement security policy are information technology personnel. Surveying the actors of the action situation under analysis is an efficient means of understanding the institutions that govern that action situation.

[21] Recall the intrusive nature of security surveys and interviews are a concern for researchers (Fulford and Doherty 2003; Knapp et al. 2007; Kolkowska and Dhillon 2013; M. T. Siponen and Oinas-Kukkonen 2007).

4.4.4 Interviews

In order to understand the outcomes, a researcher must "discover the rules being used" (E. Ostrom 2008a). Interviews of individuals responsible for managing the cyber security policy process provided details regarding the structure of the action situation, the CSP rules, and the actors that heavily influenced the process. A semi-structured interview protocol was developed (Appendix G). The survey instrument helped identify either exogenous factors or other institutional statements as a means of identifying reasons for variance. I tailored Interview questions if the case survey responses and policies required clarification.

4.4.5 Field Notes

Field notes provide "a running commentary" of the research process and provide a means of overlapping data analysis with data collection (K. M. Eisenhardt 1989). Overlapping the two activities provides a head start on analysis and can provide a quicker reaction to the need to adjust data collection efforts due to insights from the field research (p. 539). Field notes were captured within a word document for each month of the research effort. I reviewed these notes for data relevant to each case prior to construction of the case study report.

4.5 Data Management

Yin stresses important principles that support a quality case study project. First, the researcher should construct a case study database with a chain of evidence demonstrating the connections between the questions asked, the data collected, and

the conclusions drawn (Yin 2009, p. 98). The data management plan for this project follows Yin's principles.

The researcher downloaded policy documents from the unit websites, if available, and placed within data folders identified with each USG unit studied. If paper copies are provided, those are scanned and placed in digital folders.

I recorded each interview, securing each digital file in secure locations. An assistant transcribed the interviews using Microsoft Word. Each document was tagged to identify the USG unit and personnel interviewed.

Each document received a unique document number and tracked in a database developed for the project. The analyst links institutional statements to the document using the document number. Data is backed up regularly using Dropbox™ for automatic backups and thumb drives for offsite, weekly backups.

The analyst maintained a daily resource journal that served as a means of recording context, maintaining a diary of actions and notes regarding analysis, and field notes that can be used to reconstruct events if needed.

I collected, stored, and analyzed data using a number of tools. Each tool generated its own files that were included in the daily backup rituals. Much of the data collected was kept in a relational database managed by Microsoft Access. Access provides tools that document the database, its structures, and the procedures written to manipulate data and create tables for analyses. I integrated simple tables created by Access and analyzed by Excel into the study. I use "R" to create frequency and cross-tabulation tables.

4.6 Data Analysis

Analysis of the survey data required the fewest steps as I was not attempting to infer or derive data using statistical models. Interview analysis identified information that added to a process description or provided institutional statements that further specified the structure of each Knapp process. I was able to process the interview data in the same manner as the document data once this reduction was achieved.

Processing the documents was a time-consuming and tedious affair. The heart of the analysis lay in the "parsing" of the documents into the individual units of observation. Those observations were then parsed into the grammar components identified by the Institutional Grammar Tool. Additional coding tagged each observation with an appropriate identification for policy components, Knapp action situation, actor categories, and other variables of interest.

This section of the chapter provides detail for each of the procedures used to organize, analyze, and interpret the data. First, I will discuss the distinction between "units of observation" and "units of analysis".

4.6.1 Units of Analysis

The concept, unit of analysis, refers to "the entities under study and to the level at which data are analyzed and generalizations made" (Singleton, 1999 cited by Basurto et al., 2010). The research question determines the unit(s) of analysis (Yin 2009). The case, the university, is the unit of analysis. This study examines and compares the structure of policy governance of each of the four universities selected as cases to

understand how differences in the governance structure may explain differences in the policies created by the respective cases.

The structure of policy governance and policy is operationalized as a configuration of actors and institutions that regulate the decisions and behaviors of those actors. Much of the analysis will be spent on the sentences found in policy documents and interview transcripts that represent the institutional elements critical to defining and understanding structure. Each of these statements are treated as a 'unit of observation'. The concept refers to data aggregated to draw conclusions about the unit of analysis (Basurto et al. 2010b, 537). The institutional statements to be analyzed are contained in one or more policy documents that, in aggregate, create the policy and governance structures of the cases under study. The aggregation of the institutional statements provides a more granular, and perhaps more precise, means to analyzing the outcomes of the policy and governance processes of interest (Basurto et al. 2010b, 524).

Two methods are described that aggregate institutional statements into units of analysis. Nested analysis allows the analyst to aggregate multiple statements by sorting those statements by shared grammar components such as a common attribute, aIm, or aIm topic (Basurto et al. 2010b). The logic used to link the observations must be justified by the researcher (Basurto et al. 2010b, 528).

The second method examines the statements as "rule configurations" (E. Ostrom and Basurto 2011). Rule configurations represent the network of institutional statements that govern an action situation. These statements are categorized into types according to the action situation element that the rule is intended to affect (Table

4-4). Within the rule types, an analyst may identify topics, goals, and other criteria that categorize the statements within the rule type. The matrices that are produced by this method provide a means to observe the evolution of institutional configurations across time, organization, economic sector, and other constructs[22]. This study employs rules both nesting and rules configurations in its analysis.

Table 4-4 Rule Types

Type of Rule	Regulated Component	Description
Position	Positions	Title of position; Number of actors in a position; quorum level;
Boundary	Participants (Actors)	Define (1) who is eligible to enter a position, (2) the process that determines which participants may/must enter positions, and (3) how a participant may/must leave. Some rules may spell out eligibility for participants
Choice	Actions	what an actor must, must not, may, may not do based upon Conditions at the time of decision - Choice rules affect the total power created in an action situation Choice rules determine the decision tree linking actions to outcomes
Aggregation	Control	whether one individual decides, or votes of several aggregate to decide Determines the level of control an actor given a position may exercise over the selection of an action
Information	Information	Affects level of information available to participants; limits topics to be considered; frequency and accuracy of communication, legitimate channels of communication, language
Payoff	Costs/Benefits	Assigns external payoff/sanctions to particular actions Creates incentives and deterrents for action
Scope	Outcomes	Defines the range of acceptable outcomes permitted. Also limits actions linked to the outcomes.

Source: Adapted from Crawford and Ostrom (2005, 191) and Ostrom (2011)

During the early analysis of the cases, I found that each case relied upon a policy design methodology that was distinct from the other cases. These design methodologies included the AGILE software development methodology, ISO 27002 Security Standards, and a policy model developed by the Association of College and

[22] A full discussion of rules configurations is provided in Chapter 3.

University Administrators (ACUPA). I acquired documentation that outline the process for each methodology and processed those documents in the same manner as the policy documents acquired from each case. The institutional statements identified in those policy design standards were included as meta-policy statements for each case.

The design methodologies are complimentary to the Knapp model while providing more details as to specific tasks or steps the organization included as part of the policy process. The discrete steps become the "rows" of the matrix used to present the rule configurations ("columns") for each step. The entire matrix describes the rules structure for the governance processes used to develop, implement, and review policy for each case.

4.6.2 Data Coding

Once collected, the key variables for the study were coded. Responses to surveys did not require coding, but did serve as clues for matters to explore more deeply within the case interviews. The interpretation of the data collected from documents and interviews into key variables consumed most of the effort.

4.6.2.1 Surveys

The survey received a total of 3 responses from the case campuses. The response rate, while not surprising, was disappointing. Security officers are known to be reticent to reply to surveys (Knapp et al. 2007; Kolkowska and Dhillon 2013; M. T. Siponen and Oinas-Kukkonen 2007). I did use "cues" from survey responses to prepare for interviews.

4.6.2.2 Interviews

Interviews were conducted in person and via telephone following the protocol developed (Appendix G). I obtained signed, voluntary consent, from each of the interviewees. The interviews were recorded with the permission of the participants. A total of 4 interviews were conducted with 8 persons participating. The interviews were conducted by case (Table 4-5).

Table 4-5 Interviews Conducted

Case	Participants (Titles)	Length	Dates
Georgia State	1 CISO	53 mins	23 Mar 2012
Georgia Tech	3 CISO; Compliance Manager; Dir. Of Compliance, Office of Enterprise Risk	45 mins	22 Mar 2012
UGA	1 CISO	50 mins	23 Mar 2012
Georgia Southern	2 CIO, CISO	50 mins	13 Apr 2012

The transcribed interview was edited into an annotated version of the interview with a focus on extracting statements relevant to the categories of actions and rules that the research model suggested. This version of the interview was processed in the same manner as other documents so that institutional statements could be identified, coded, and categorized by the process where those statements were employed.

4.6.2.3 Documents

Most of the documents analyzed were policy documents obtained from the cases. Other documents include the annotated interviews and significant external policy standards, mandates, and design methodologies. "Other" documents are

referenced by the cases in two ways. Most were referenced within the information security documents obtained. The remainder were identified through the interviews as a set of institutions integrated into the case's policy process.

The meta-data for each document was captured as part of the inventory process discussed in the document protocol (Appendix C). The entire set of documents (policy, interview, external policies) were complete, each document was dissected, employing methods developed as part of the Institutional Grammar Tool (IGT), to capture the institutional statements that are the units of observation for this study.

Institutional Grammar Analysis

Much research has focused on how policy should be structured while very little work has been done with regards to the content of policy (Baskerville & Siponen, 2002; Dhillon & Backhouse, 2001; N. Doherty, Anastasakis, & Fulford, 2009). Policy content provides observable data that can measure differences between "policy as implemented" against "policy as mandated or suggested". Document analysis of published policies provides an inventory of formal rules, norms and standards. Interviews of actors engaged in the respective action situations provide an additional source of rules, formal and informal, relevant to the policy process. The deconstruction of these statements into their respective types (norms, strategies, and rules) and elements provides a granular level of data from which an analyst may observe the effects of governing institutions upon policy outcomes.

A clear categorization of the components of policy or institutional statements is critical for policy analysis (S. Siddiki et al. 2011, 79). The IGT provides guidelines to 1)

identify institutional statements; (2) code institutional statements; and (3) conduct a nested analysis of institutional statements (Basurto et al. 2010b, 524). The IGT reveals the actions permitted; the objects of the actions; the conditions for those actions; and the sanctions/incentives. Applied to analysis of policy documents, IGT gives the analyst a more robust and rigorous understanding of both scope and structure of policy. The IGT enables analysts to investigate:

1) The effects of configurations of institutional statements;
2) The consistency and completeness of institutional statements;
3) Legitimacy and compliance of institutional statements (Crawford and Ostrom 1995, 595).

Crawford and Ostrom define the grammar of institutional statements as a syntax expressed in a format called ADICO: Atrributes, Denotic, aIm, Conditions, Or else (1995, 584). An institutional statement is composed of:

Attributes : a variable which identifies the actor, or position, to whom the statement applies.
Deontic : a variable which contains the modal verb defining what may be permitted, required, or forbidden.
a**I**m: variable describing the actions or outcomes to which the deontic is assigned. The action or outcome must be physically possible. The negation of the action or outcome must be possible as well.
Conditions : a variable defining when, where, how and to what extent the aIm is allowed per the Deontic
Or else : a variable defining the sanctions to be imposed for not following the rule.

Siddiki and others suggest a sixth component of the syntax, the oBject, is needed to separate those responsible for carrying out the aIm and those receiving the aIm

(2011, 87). The oBject provides clarification as to the intended receivers of policy actions. Mapping the intended policy action to a specific recipient provides a measure of policy clarity used to test policy effectiveness.

Basurto and others found that the definition of the Attribute supplied by Crawford and Ostrom (1995) is ambiguous. The statement AIM has both an actor creating the action and an actor receiving the action causing confusion as to which actor is the focal actor (Basurto et al. 2010b, 525). Siddiki and others argue that the concept of oBject distinguishes between the actor responsible for the action and the actor receiving the action. Statements that do not explicitly name the Attribute often identify the oBject. Context then determines the Attribute.

Knowing to whom the responsibility for executing an action is given improves the specificity of our mapping of institutions, interactions, and actors. Such specificity enhances the explanatory power of the Knapp model, and provides a firm foundation for future research questions that focus on actors, their qualifications, their networks, and their positions of influence within organizations. For this purpose, I categorized the Attributes of policy to identify Top Management, Individuals, Vendors, and the Organization as primary actors.

IGT Analysis of Cyber Security Policy Documents

A number of recent studies employ the grammar tool as a method for reliable data collection and analysis (Carter et al. 2013; S. N. Siddiki 2013; Feiock et al. 2014). One study (Basurto et al. 2010b) has proposed guidelines to:

1. Identify institutional statements;
2. Code institutional statements as strategies, norms, and rules; and

3. Conduct a nested analysis of the coded institutional statements

The protocol for coding the statements observed in the documents is found in Appendix H. Every statement within the document is assigned a sequential number identifier. The statements were broken into their grammatical ADICO components. Once those components were separated, the observed statement was coded for the following variables:

Table 4-6 Statement Variables

Variable	Description
Category (of Attribute)	Is the actor Organization, Top Management, Individual, Vendor
Deontic Class	Is the action Required, Permitted, Forbidden
ACUPA	Statement assigned to what step within the ACUPA methodology.
ADICOB2 sequence	What ADICO elements are present
Policy type	Is statement part of a Meta-policy, Policy, Standard, Procedure, Guideline, or ancillary
Statement Type	Is the statement a Strategy, Norm, Rule, Definition, External Policy reference, Objective Definition, Outline indicator
Rule Type	Following the definitions found in Table , is the statement a rule that belongs in the category of: Aggregation, Boundary, Choice, Information, Payoff, Scope
Governance Action Situation	The statement applies to which Knapp process?
CyberSec Action	The statement applies to which USG required policy area?

4.6.3 Nested Analysis

Policy documents represent a collection, or aggregation, of institutional statements. It is the aggregate nature of those statements that creates the decision-making situation that governs individual and collective behaviors. Nesting those statements provides a means of understanding the structure of those situations.

4.6.3.1 Nested analysis of the coded institutional statements

The method proposed to identify variations in policy governance requires a means of cataloguing and measuring the combination of institutional statements and the interactions of those statements with actors as structures that define action situations identified by Knapp as requisite for create effective security policy. One research paper employed a method to "nest" institutional statements in order to "…help understand the constraints and opportunities of individuals in a particular action arena" (Basurto et al. 2010b, 524).

The Knapp Action Situations (Table 4-7) represent the various processes identified by practice and theory as necessary for an organization to create effective information security policies. Organizing these statements within those defined processes "…clearly conveys meaning" (Basurto, et al, 2010, 528).

Table 4-7 Nested Analysis - Example

Action Situation	Rule Type	Section Level	cstate
Review	Boundary	1. Issue Identification & Scope Definition	identify [I] Policy issues [B] [at all times] [C] [Obs: 336 , 3]
Development	Boundary	1. Issue Identification & Scope Definition	identify [I] Policy issues [B] [at all times] [C] [Obs: 336 , 3]
Review	Choice	1. Issue Identification & Scope Definition	determine [I] who is or should be affected by policy issue [B] [at all times] [C] [Obs: 336 , 4]
Development	Choice	1. Issue Identification & Scope Definition	determine [I] who is or should be affected by policy issue [B] [at all times] [C] [Obs: 336 , 4]
Review	Choice	1. Issue Identification & Scope Definition	define [I] scope of the issue [B] [at all times] [C] [Obs: 336 , 5]
Development	Choice	1. Issue Identification & Scope Definition	define [I] scope of the issue [B] [at all times] [C] [Obs: 336 , 5]
Review	Choice	1. Issue Identification & Scope Definition	determine [I] existence of policy [B] if policy exists [C] [Obs: 336 , 6]
Development	Choice	1. Issue Identification & Scope Definition	determine [I] existence of policy [B] if policy exists [C] [Obs: 336 , 6]
Development	Boundary	1. Issue Identification & Scope Definition	assign [I] focal points [Officers of Primary Responsibility (OPR) and Officers of Coordinating Responsibility (OCR)] [B] [at all times] [C] [Obs: 336 , 8]
Development	Choice	1. Issue Identification & Scope Definition	assign [I] focal points [Officers of Primary Responsibility (OPR) and Officers of Coordinating Responsibility (OCR)] [B] [at all times] [C] [Obs: 336 , 8]
Development	Boundary	1. Issue Identification & Scope Definition	assign [I] Focal Points - Officers of coordinating Responsibility (OPR) Most of the time this will be the IT Director [B] [at all times] [C] [Obs: 336 , 9]
Development	Choice	1. Issue Identification & Scope Definition	assign [I] Focal Points - Officers of coordinating Responsibility (OPR) Most of the time this will be the IT Director [B] [at all times] [C] [Obs: 336 , 9]
Development	Information	1. Issue Identification & Scope Definition	deliver [I] Memoranda [B] regarding Statement of Policy Need [C] [Obs: 336 , 10]

Key: A – Attribute, I – AIM, C – Condition, B – oBject. Observation – Doc ID, Unit of Observation

4.6.3.2 Analyzing Action Situation Structure with IGT

The nesting analysis method, described by Basurto and others (2010), suggests that one means of testing for complementary values and structures within and among institutions is to compare the goal (or aim) of the institutional statements. The Knapp model conceptualizes structure as a set of processes, individually defined, whose outcomes and outputs create interaction among the institutions and actors within each process. That interaction is the linkage that creates a structure for policy.

Ostrom and Basurto (2011) describe a process of identifying configurations of rule types to define action situation structures. The authors inventoried rules from studies of irrigation systems and found within boundary rules (noted as B in their rule

matrix), one can categorize them as focused on the use of the objects of Land (B1), Shares (B2), and Membership (B3) to define entry and exit to the action situation. Those sub-types are measured by strength of the deontic (S, N, R). The resulting observations (Figure 4-5) are assembled, for their purposes, in a matrix where each row symbolizes a point of time and the rule type observations symbolizing the rule configurations at that time (E. Ostrom and Basurto 2011, 328).

Table 3. Rule or norm configuration inventory

Potential Rules or Norms	Boundary			Position			Choice (Allocation)			Aggregation			Information			Payoff			Scope		
	B1	B2	B3	P1	P2	P3	C1	C2	C3	A1	A2	A3	I1	I2	I3	Y1	Y2	Y3	S1	S2	S3
Configuration T1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Configuration T2	S	0	0	0	0	0	0	0	S	0	0	0	0	0	0	0	0	S	0	0	0
Configuration T3	S	0	0	R	0	0	0	0	R	R	0	0	0	0	0	R	0	S	0	0	0
Configuration T4	S	0	0	R	0	0	P	0	0	R	0	0	0	0	0	R	0	S	0	0	0
Configuration T5	R	0	0	R	0	0	P	0	0	R	0	0	0	0	0	R	0	S	0	0	F

Figure 4-5 Configuration Inventory (Ostrom and Basurto 2011, 328)

Two particular types of policies are: a) meta-policies that govern information security policymaking and b) acceptable use policies that govern the behavior of individuals and organizational. A nested analysis of institutional arrangements yields a matrix that highlights the rule structure as shown in Table 4-8. This table shows the most granular configuration of rule types within each of the governance action situations predicted by the Knapp model as necessary to promote effective policy governance.

Table 4-8 Analysis of USG 11.3

Knapp Action Situations	Statement Type	Total Statements	Aggregation	Boundary	Choice	Information	Position	Scope
Policy Awareness and Training	N	4				2		2
Policy Development	N	10	1		3	2		4
Policy Enforcement	N	2			2			
Policy Implementation	N	5			4		1	
Policy Review	N	9			2	3		4

Rules from the USG are combined with the institutional statements of the USG unit that represent the policy component described as meta-policy. This creates the unique set of rules that govern policy making for that unit. A matrix such as Table 4-8 will vary according to the differences in unit statements added at the time of analysis. A comparison of a policy type (such as Acceptable Use) across multiple organizations is shown in Table 4-9. The table allows us to see rule configurations vary within Knapp action situations across multiple organizations. From this level of analysis, we can identify opportunities to explore further detail as directed by the hypotheses.

Table 4-9 Comparing Rule Configurations Across Orgs

Knapp Governance Action Situations	Org	Type	Total	Aggregation	Boundary	Choice	Information	Payoff	Position	Scope
Awareness and Training	Ga Southern	N	2				2			
Development	GT	N	3	2			1			
Development	GT	N	3			1				2
Development	USG	N	15			7				8
Development	USG	R	2					1		1
Enforcement	Ga Southern	N	18		2	5	6	5		
Enforcement	Ga Southern	R	1					1		
Enforcement	GT	R	1					1		
Enforcement	USG	R	1					1		

4.7 Interpreting Data

Given the eccentricities of the IAD framework and the tools of analysis employed, the ability to discern the forest from the trees is an important obligation for which the analyst is responsible. At the end of the day, what does all this data mean?

The governance structure is defined by the actors and the rules assigned to each process designed to create, retire, and modify policy in alignment with organizational goals. Policy structure may be defined as the relationships between the objectives of policy and the policy elements available to achieve those objectives. Analysis of the date examines the components of policy, such as guidelines, standards and procedures, that are written to delineate responsibilities and actions needed to affect outcomes. The scope of issues addressed by the policy can be identified to understand what areas of concern are covered by policy. The form of language used to communicate policy indicates to whom and for whom the policy is written to be understood. And the fit of that policy relative to the organizational structure and culture carries implications as to whether the policy serves the organization practically. Taken together, these elements provide metrics of structure that correlate with the likelihood of policy effectiveness.

4.7.1 Governance Structure

The measure of governance structure is operationalized by identifying actors and institutions within the Knapp action situations. A simple crosstab of statements sorted by action situation and Attribute Category shows the distribution of actors (Organization, Top Management, Individual observed in those situations. Statements

identified as “meta-policy” statements, those that are the rules guiding how policy is made, are the focus of this analysis. The main features of the governance structure are presented by counts that indicate which institution types are distributed across the action situations of interest. An example is found in table 4-10.

Table 4-10 Sample Analysis of Structure - Actors within Action Situations

Action Situation	**Organization**	**Top Mgt**	**Row Total**
Approval	4	3	7
	0.1	0.2	
	57.1%	42.9%	9.2%
	8.0%	11.5%	
	5.3%	3.9%	
----------	----------	----------	----------
Awareness and Training	4	4	8
	0.3	0.6	
	50.0%	50.0%	10.5%
	8.0%	15.4%	
	5.3%	5.3%	
Development	25	17	42
	0.3	0.5	
	59.5%	40.5%	55.3%
	50.0%	65.4%	
	32.9%	22.4%	
Implementation	4	0	4
	0.7	1.4	
	100.0%	0.0%	5.3%
	8.0%	0.0%	
	5.3%	0.0%	
Review	7	2	9
	0.2	0.4	
	77.8%	22.2%	11.8%
	14.0%	7.7%	
	9.2%	2.6%	
Risk Assessment	6	0	6
	1.1	2.1	
	100.0%	0.0%	7.9%
	12.0%	0.0%	
	7.9%	0.0%	
----------	----------	----------	----------
Column Total	50	26	76
	65.8%	34.2%	

The precision of analysis may be increased by "drilling down" into the detail. Understanding the policy making processes using the ACUPA methodology give the analyst an opportunity to look at more discrete action situations located within a Knapp process. For example, eight of the nine boundary rules that determine entry to action situations are employed to formally identify who may be appointed to the team (Table 4-11).

Table 4-11 Rule Configurations within ACUPA Steps

Action Situation	Step	Actions	Aggregation	Boundary	Choice	Information	Payoff	Position	Scope	Grand Total
2. Conduct Analysis	2.01	Identify Owners	1	0	1	1	0	0	0	3
	2.02	Determine Path (Policy Plan – Scope Definition)	0	0	1	0	0	0	0	1
	2.03	Assemble Team	0	8	0	0	0	0	0	8
	2.04	Gather Data	0	0	0	0	0	0	0	0
	2.06	Determine Risks	0	0	0	0	0	0	0	0
	2.07	Determine Stakeholders	0	0	0	1	0	0	0	1
	2.08	Determine solutions for the problem/need	0	0	2	0	0	0	0	2
	2.09	Determine if present policy can be revised	0	0	0	1	0	0	0	1
	2.1	Determine need for new policy	0	0	0	0	0	0	4	4

Normalization of the organizational positions referenced by institutional statements provides clarity as to which actors participate across the case organizations. Table 4-12 categorizes actors into common positions and shows how they may be

required, or not, to participate, in the policy making structure. The specificity of how those actors may be compelled to participate is provided by the quality of the boundary rules identified for each case. A 1st order boundary rule is one that specifically requires participation of a particular actor. A 2nd order rule, an invitation, is one that makes participation one that is at the will of the actor and not necessarily a decision that is institutionalized.

Table 4-12 Actors and the Boundary Rule Types

Actor	**Georgia Tech**
President	1st Order – USG
CIO	1st Order
CISO	1st Order
Legal Affairs	1st Order
Internal Audit	1st Order
Faculty and Research	Invite CISO/CIO
Bursar	Invite CISO/CIO
Extended Campuses	Invite CISO/CIO
Finance	1st Order
Human Resources	1st Order
Public Affairs	
IT – Policy Compliance	1st Order
Registrar	1st Order
IT – Enterprise	1st Order
Subject Matter Experts	1st Order
Policy (Process) Owners	Invite CISO/CIO
Stakeholders	Invite CISO
Others	Invite CISO

A determination of the relative formality of the governance structure is made using the criteria in Table 4-13.

Table 4-13 Criteria for Determining Type of Governance Structure

Knapp Governance Structure		**Policy Structure**		
Action Situation	Description	Ad Hoc	Informal Network	Formal Network
Approval	Actions required to approve policy; to operationalize the policy	W	W	P
Development	Activities include issue identification, definition of scope, research and analysis and stakeholder input	W	P	P
Retirement	Removal of policy from active service	N	W	P
Review	Management review of policy performance, alignment with business objectives, and effectiveness given other emerging technologies and security issues	N	W	P
Risk Assessment	Identification of organizational values, policies that may be compromised if certain behaviors are allowed to occur	N	W	P
Legend: (P)resent; (W)eakly Present; (N)ot Present				

4.7.2 Policy Structure

An analysis of the distribution of statements by the type of policy component represented by the statement, shows how documents may focus on management or individual users (Table 4-14).

Table 4-14 Sample - Distribution of Policy Components Per USG Requirement

Document	Ancillary	Guideline	Procedure	Standard	Policy	Meta-policy	Tot Obs
Computer Usage and Security Policy [343]	0	18	37	46	50	6	157
Credit Card Processing [348]	0	1	15	15	31	4	66
Data Access Policy [344]	0	0	18	8	10	2	38
Information Security Exception Policy [353]	2	0	1	0	2	18	23
Interview with GT CISO [476]	0	0	22	1	0	1	24
Policy Exception Procedure [359]	0	0	0	0	0	34	34
Policy Review Process [360]	0	0	0	0	0	11	11
Total Obs	2	19	93	70	93	76	353

A cross-tab analysis examines the distribution of statements identified by components (Table 4-15).

Table 4-15 Analysis of Components with Policy Documents

Document	Ancillary	Guideline	Procedure	Standard	Policy	Meta-policy	Total Obs
AGILE Software Development Principles [473]	0	0	0	0	0	11	11
Appropriate Use of Telecommunication Services Policy [338]	1	0	0	5	1	1	8
Compliance with the Higher Education Opportunity Act Peer-to-Peer File Sharing Requirements [330]	0	0	22	6	4	0	32
Data Stewardship and Classification [325]	1	3	45	16	20	0	85
Incident Response Procedures [331]	0	3	17	4	4	0	28
Information Technology Appropriate Use Policy [332]	0	1	24	51	31	3	110
Interview Analysis - Table of Rules [474]	0	0	0	0	0	10	10
IT Policy Development & Review Process [336]	0	0	4	2	0	45	51
Protection and Security of Records Policy [337]	0	0	2	1	2	0	5
Workstation management policy [341]	0	0	1	0	8	0	9
Workstation Management Standard Procedures [342]	0	3	20	15	5	0	43
Total Observations	2	10	135	100	75	70	392

An organization's policy structure, using Doherty's taxonomy, is defined by the types of documents found within each policy area Table 4-16.

Table 4-16 Criteria to Determine Policy Structure

Criteria – Document Structure	Ad Hoc	Informal	Formal
General Info Sec policy present	Yes	Yes	Yes
Number of related documents present	Yes	Yes	Yes
Documents reference existing policies	Maybe (few)	Yes	Yes
Vertical links, few horizontal	Few	Yes	Yes
Policies and standards present – each focused on specific area	Maybe	Yes	Yes
Horizontal links present	Maybe a few	Yes	Yes
Meta policy present	No	Maybe	Yes
Criteria – Knapp Structure			
Awareness and Training -	Weak	Yes	Yes
Implementation	Few	Yes	Yes
Monitoring	None	Maybe	Yes
Enforcement	None	Weak	Yes

Legend: (P)resent; (W)eakly Present; (N)ot Present

4.7.3 Structure as Networks

Graphing the relationships among the policy documents provides a visual confirmation of the decisions made regarding structure. The stated purpose of each document, along with an analysis of the distribution of statements as policy components, classifies each document which is given a shape. Connections are made by references between these documents.

4.7.4 Case analysis

The unit of analysis for this study is the case. The case defines the context within which the policy statements analyzed are constructed. Analysis of each case was a continual exercise.

4.7.4.1 Early Analysis

One of the strengths of qualitative research is the rich data the analyst is able to observe. "Early analysis" is strongly suggested by Miles and Huberman (1994, 50) to energize field research, helping the analyst to "think about existing data and strategies for collecting new, often better, data". Working with the data from the early attempts to capture survey responses, interviews, and document analysis provided opportunities to identify improvements to the research protocol. I noted improvements in the research journal and updated the protocol. This necessitated multiple data collection and analysis with the initial targets of study but improved the quality of the research overall.

4.7.4.2 Within Case Analysis – Case Reports

Writing up the observations of a case is the typical first step of case analysis (K. M. Eisenhardt 1989, 540). The case report helps the analyst to cope with the volumes of data that generally accompany case studies (Miles and Huberman 1994, 84). The act of summarizing and analyzing the data for the case within a structured report is a process that enables the analyst to become intimate with the case, to identify patterns unique to each case and to develop knowledge necessary to develop cross-case comparisons (K. M. Eisenhardt 1989, 540).

The conceptual framework, research questions, hypotheses, and sampling plan determine the case outline (Miles and Huberman 1994, 84). The outline defines a structure where data will be placed and analyzed; and provides the analyst with a map that includes data displays and narratives for each group of data collected (Miles and Huberman 1994, 84). This map provides the analyst with a means of assuring consistent data capture and analysis for each case. Sharing the case report with the subjects provided important feedback necessary to the reliability and accuracy of data collected for each case (Miles and Huberman 1994, 85). Case reports provide focus and efficiencies for data analysis and improve the reliability of that analysis for multiple case studies (Miles and Huberman 1994, 84).

The initial work spent creating an outline is in itself a process that forces the analyst to review the research questions, the research framework, and the hypotheses. The analyst can observe how best to display data collected and whether the research protocol has considered the elements needed to complete the case analysis. In this

study, each report begins with an overview of the case, its environment, and data that describe the external and internal factors of that USG unit. The data analysis for each case broke into two sections: policy governance and analysis of the acceptable use policy. The order of hypotheses presented in chapter three organizes the data analysis for each section. The case report concludes with a summary of the findings of that case and notes regarding items for further research. An appendix provides annotated descriptions of the policy documents analyzed, the survey data for that unit, and a summary of the interview data collected.

4.7.4.3 Cross-Case Analyses

Case reports present the data found by observing each case (within-case analysis) and the data created when those observations are compared against other cases (cross-case analysis). Eisenhardt suggests a tactic of selecting key categories of factors to observe patterns of behavior via cross-case analyses. Cross-case analysis provides an opportunity to observe whether individual factors affect the expected governance structures and policy outcomes for USG units(K. M. Eisenhardt 1989, 540). These observations may consider the effects of these factors more succinctly by observing pairs of cases that are more similar and more different. The case selection strategy for this study supports this tactic. Cross-case analyses improves the likelihood that subtle effects within the data may be found (K. M. Eisenhardt 1991).

4.8 Data Validity and Reliability

The methods employed, use of IGT, survey tools, and interview techniques have a rich history in the literature. The structure and robustness of IGT provides a strong,

reliable approach to identifying policy designs that can be mapped to the policy areas being attacked. When possible the study has relied upon external measures of categories (e.g. Carnegie Classification) enhancing the potential for more reliable generalizations across the higher education sector. This study builds upon and expands recent studies exploring the relationship between configurations of institutional arrangements as they affect policy design and policy implementation.

4.8.1 Construct Validity

Yin elegantly summarizes the four tests used to assess the quality of a research design (2009, 40-41). Construct validity can be demonstrated if concepts are operationalized using approaches demonstrated by other, similar studies. For this study, external sources will justify the operationalized concepts employed. Multiple sources of evidence will be derived from published statements, interviews and surveys. Finally, I propose allowing key actors within each case review the unit data reports for omissions and errors.

4.8.2 Internal Validity

Internal validity refers to the strength of the design of the study to account for alternative explanations or spurious effects which may otherwise account for the phenomena under study (Yin 2009). In order to address this test, this study has surveyed the literature to identify models and frameworks that have accounted for spurious effects to the extent that present knowledge allows. Triangulation of data from documents and interviews will be used to demonstrate convergence of concepts.

Comparison of data across unit classifications will test the strength of institutional models versus traditional explanations such as contingency theory. Rival explanations, such as a network theory of governance, are discussed within the analysis. The use of best-worst case analysis both within and across categories provides a test of the strength of inferences drawn from this study.

4.8.3 External Validity

External validity is the likelihood that the findings of this case study may be generalizable beyond the study. The study design builds upon recent studies, using models and frameworks developed using diverse approaches such as grounded theory, action research, and institutional analysis. These multiple approaches provide a foundational framework which supports development of several theories, particularly institutional rational choice theory, as applied to wicked problems. Cyber security is a type of wicked problem. The hundreds of studies produced by researchers employing the IAD framework point to an area of study where generalizable results may be applied. By extension of logic, a study of how institutions affect policy processes which manage cyber security problems may produce findings from which inferences or implications are drawn to advance studies of other wicked problems.
Selection bias – truncating – seriously alters our ability to generalize our findings.

4.8.4 Selection Bias

Analysts should be aware that selection bias may lead to an observed correlation between the causal variable(s) and the outcome that is weaker than would be if the full

population were analyzed. This effect is similar to that observed in regression analysis using truncated data which leads to the analyst underestimating the strength of the causal variables in the truncated sample (Collier and Mahoney 1996, 66). Small-N studies such as this one are prone to the effects of selection bias. However, Collier and Mahoney specify that when using pair-comparison to select the cases studied, the important test is whether the analyst has used the full range of variation of the outcome studied when selecting the cases of both extremes [p. 67]. In this study, we have selected USG units that are compliant and non-compliant and exhibit variation in the causal variables such as size and mission. Examination of cases within the more narrow groups and across the groups thus allows the analysis to reasonably manage effects of selection bias while compensating for possible loss of parsimony, accuracy and causality. This study analyzes cases within comparative groups of USG units, as established by their respective Carnegie classifications. Examination of cases within the more narrow groups and across the groups thus allows the analysis to compensate for possible loss of parsimony, accuracy and causality and maintain integrity in relation to generalizability of results.

4.8.5 Reliability

Reliability is a quality of design which assures us that if another researcher follows the same methods and procedures the likelihood of replicating the results of this study are quite good. This study will follow an established research protocol with each action step aptly described. A research journal will capture highlights of the effort as time progresses.

4.9 Limitations

Information security research causes many organizations to distrust external researchers (N. Doherty et al., 2009) because the research is viewed as "one of the most intrusive types of organization research" (Kotulic and Clark 2004). The statistics for reported incidents at US-CERT show that despite the predominance of cyber assets in the private sector, reports of incidents from that sector lag behind incidents reported by public sector entities.

Social demand bias occurs when subjects of interviews, like the semi-structured interviews proposed here, believe it is "politically incorrect for subject to indicate they believe security was unimportant" (Ramachandran, Rao, and Goles 2008, 9). IT professionals have admitted a "bias towards performance over security when working under pressure" (Ramachandran, Rao, and Goles 2008, 10). Triangulation of data collected from the survey, documents, and interview can highlight examples of such bias. But, such bias may be evidence of the very "norms" that regulate the policy process. As such, that bias cannot be directly dismissed without considering the possibility that data is being omitted in a fashion that will adversely affect the outcomes of the study.

The investigator of this study has been an employee of the University System for 10 years. A significant portion of that time was spent as a special advisor on policy for the USG CIO. Bias is objectively an item of concern. On the other hand, the investigators knowledge of process and technology brings strengths to the study and

also facilitates confidence with respondents answering surveys and interviews as the investigator has material knowledge of their area of expertise.

As this study is an exercise to satisfy requirements of a dissertation, the study was unable to employ multiple coders to manage possible coding biases. Thus coding reliability is a real concern that can only be addressed by introducing additional coders to test and manage such bias.

The study is an exploratory comparative case study. As such, the findings are limited to the cases observed. A number of means are presented that are used to classify observations. The reliability and validity of those classification methods can only be substantiated by replication in other studies. I identified and placed those observations within action situations thought to model the actual processes employed by the cases studied. Additional research is needed to validate those classifications. For this study, the validity rests upon the prima facie evidence presented.

Ostrom (2007,22) believes that at any one level of analysis, combinations of rules, attributes of the world, and communities of individuals involved are combined in a configured, rather than an additive manner. The small n of this study limits any attempt of combinatorial analysis. This aspect of institutional analysis is an important goal of future research that can lean upon the data collection framework validated in this study to gather a larger sample of higher education organizations from which such analysis may yield results of statistical significance.

I noted in the introduction caution that the tool may not eliminate all ambiguity regarding identification of components or classification of statements (Crawford and

Ostrom 1995, 583). Identification of statements critical to analysis and the appropriate level of precision "…are important research design questions in institutional analysis analogous to specifying the appropriate variables and precision of variables in statistical analysis (Crawford and Ostrom, 2005, 373)". Trial and error is an important part of that process.

4.10 Ethics and Human Subjects Issues

A research protocol approved by Georgia State University's Internal Review Board guided this study. Confidentiality of interviewees was not guaranteed as the roles and comments can easily be used to discern the individual involved. Further, employees of the University System of Georgia are subject to the Open Records Act and thus have limited expectations as to privacy and confidentiality.

4.11 Summary

This chapter has reviewed the logic model, the research design and methods of analysis followed to examine the research question and to test several hypotheses. Plans for managing the data collection and analysis activities were discussed, as were issues regarding the validity, reliability, and limitations of this study.

Chapter 5–External Conditions and Constitutional Level Rules

The research model expects influences external to the organization to affect the structure of the policy making apparatus for each case. In addition to the Board of Regents, the individual cases must comply with expectations of security from vendors, funding partners, and the federal government to secure all or at least portions of their information assets. In this chapter, I examine the conditions noted by the subjects of my interviews as most influential upon the policy governance for each respective case. First, I explain how the IAD descriptors and tools work within the context of this study. I then examine the external standards acknowledged as strong influences on the design of policy governance and policy statements. Finally, a summary of case descriptions provides contextual details that are important to the data analysis presented in chapters 6 and 7.

5.1 Interpreting the Data using IAD Descriptors

The Knapp model (Figure 5-1) provides high-level expectations of how an organization should structure the governance of its security processes to create and sustain effective security policy. This study treats each Knapp process as an action situation. An action situation is "an analytic concept that enables an analyst to isolate the immediate structure affecting a process of interest to the analyst for the purpose of explaining regularities in human actions and results, and potentially to reform them"(E.

Ostrom 2011). The Knapp model describes a network of action situations that both theory and practice suggest are essential to assure effective cyber security policies.

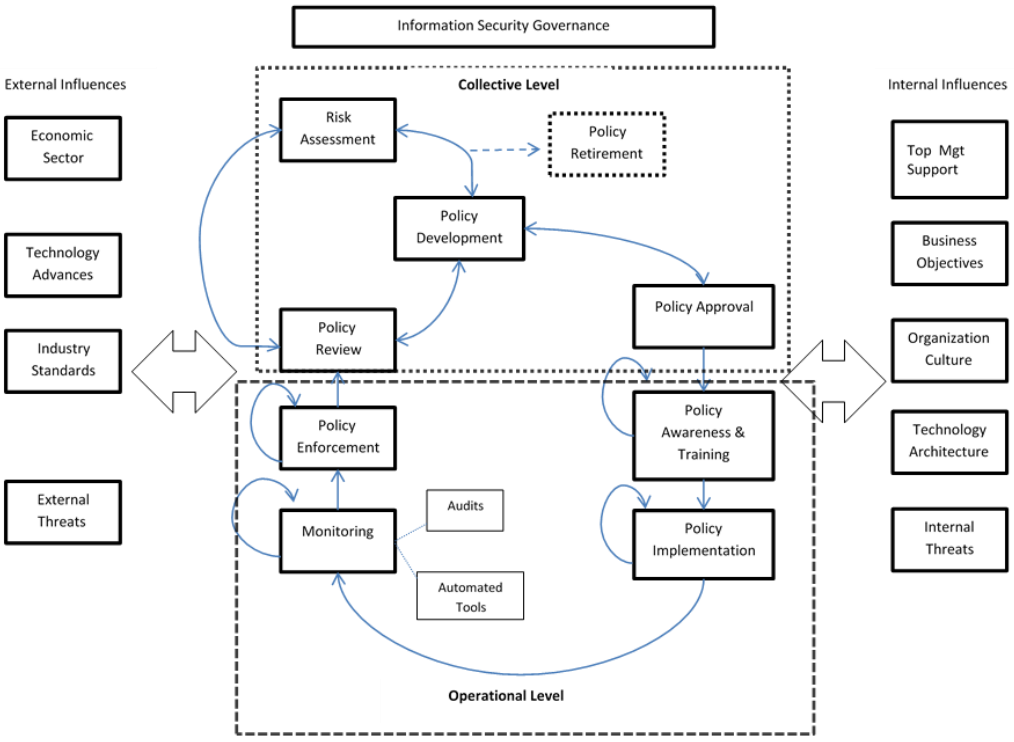

Figure 5-1 Knapp Security Governance Model

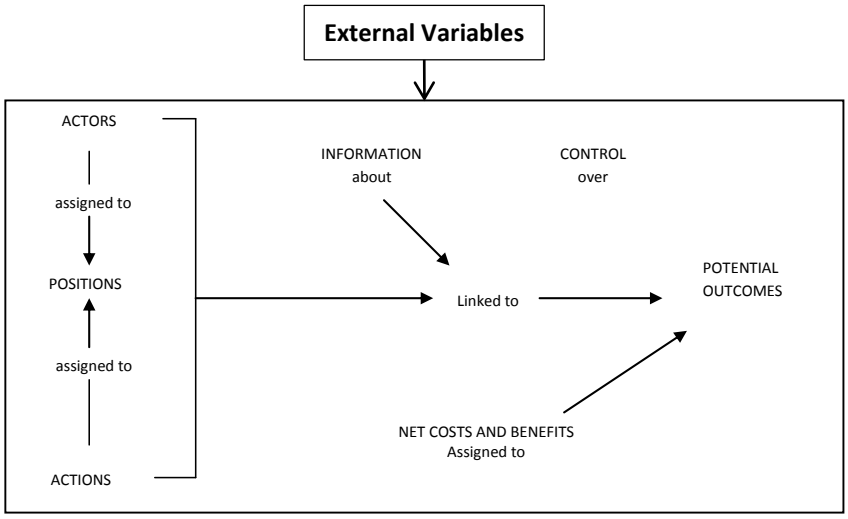

Figure 5-2 Internal Structure of an Action Situation (Ostrom 2001, 10)

The structure of each process/action situation is determined by observing and identifying the process components. Those components are described by the common set of IAD variables shown in Figure 5-2.

The IAD components and their attributes (Table 5-1) help to organize my analysis of each step in the process used by campuses to develop policy. If I am to compare how each campus develops policy, I want to know:

- **Actors** - Who participates? Are we limited to leadership (CIO, CISO) from the technology division? Is there representation from across the campus? How many?
- **Positions** - What are the positions in this process? Who calls the meetings? Who runs the meetings?
- **Actions** - What actions is this group allowed to take? Can this group formulate policy without the approval of the cabinet?
- **Control** - Can one person or any persons in this group make the decision that a policy is complete? Is a decision final or conditioned upon the decision of another policy processor processes? Is consensus of the group required?
- **Information** – What type of information is shared/not shared? Does the process of risk assessment, monitoring, enforcement provide information as to effectiveness of current policy? What kind of information does this group share with others that may have inputs to the decision of what the policy may include? What kinds of information do other sources feed to this group? Is there a connection between the information and the actions that may be taken? Is budget information shared with the group? Is information from standards organizations, the USG, federal security centers, and vendors available to the group while policy is being developed?
- **Cost/Benefits** – What incentives motivate the individual actors? The group? Are there penalties for taking ineffective actions? Are those penalties financial? Social?
- **Outputs** – what is the range of outputs expected/allowed? Are the outputs contributing to actions to make the campus aware of policy changes? Who monitors these outputs? Who measures the actual outputs against expectations (i.e. mandates)? Do these outputs contribute to the sanctions or incentives (Costs/benefits) that motivate the actors developing policy?

Table 5-1 Action Situation Components

(Table created from terms found in An Introduction to the IAD and the Language of the Ostrom Workshop, Michael Dean McGinnis 2010 and Understanding Institutional Diversity, Ostrom 200)

Component	Definition	Attributes
Actors	who evaluate actions, outcomes, outputs, and information and are assigned to	• Number • Status as individuals, team, composite actor • Individual attributes (age, gender, education, experience)
Positions	roles and titles that confer authority over the process; positions connect the actor to the action	• Role • Title • authority
Actions	Term includes overt acts and choice not to act. May be thought of as selection of a setting or value that will affect an outcome variable (Ostrom 2005 45)	• choice of a specific action • strategy – series of choices • action sets –available actions
Information	Formal representations of action situations assumes all actors have knowledge of all actors, actions, linkages between actions and outcomes, positions, information available to other players, and cost/benefit data	• Complete information – all actors know full structure of action situation • Incomplete – which actor knows what becomes important
Outcomes	Generated by product of outputs of an action situation, other closely related action situations, and exogenous influences	• Physical results • Material rewards/costs • Valuation of physical results and material rewards/costs
Control	Power over the linkage of actions to outcomes – control varies from none (0) to 1 (total). A value of 1 occurs when the probability of an action to an outcome is certain given the action.	• Likelihood of affecting outcome • Power (value of opportunity x control) • opportunity
Costs/Benefits	Rewards/sanctions distributed to actors Also Actions have costs weighed against the "benefits" of outcomes	• Outcome related – incentives assigned to outcomes as a result of actions taken • Path related – incentives assigned to actions taken to produce the outcome

The structure of an action situation is defined by the actors, and the rules and norms that represent "shared understandings among those involved that refer to enforced prescriptions about what actions (or states of the world) are required, prohibited, or permitted" (E. Ostrom 2011, 17). The rules can be typed, or categorized, by their relation to the action situation components (Table 5-2).

Table 5-2 Rule Types

Type of Rule	Regulated Component	Description
Position	Positions	Title of position; Number of actors in a position; quorum level;
Boundary	Participants (Actors)	Define (1) who is eligible to enter a position, (2) the process that determines which participants may/must enter positions, and (3) how a participant may/must leave. Some rules may spell out eligibility for participants
Choice	Actions	what an actor must, must not, may, may not do based upon Conditions at the time of decision - Choice rules affect the total power created in an action situation Choice rules determine the decision tree linking actions to outcomes
Aggregation	Control	whether one individual decides, or votes of several aggregate to decide Determines the level of control an actor given a position may exercise over the selection of an action
Information	Information	Affects level of information available to participants; limits topics to be considered; frequency and accuracy of communication, legitimate channels of communication, language
Payoff	Costs/Benefits	Assigns external payoff/sanctions to particular actions Creates incentives and deterrents for action
Scope	Outcomes	Defines the range of acceptable outcomes permitted. Also limits actions linked to the outcomes.

Source: Adapted from Crawford and Ostrom (2005, 191) and Ostrom (2011)

The seven rule types shown in Figure 5-3 help describe action situation structure (Ostrom 2011, 19).

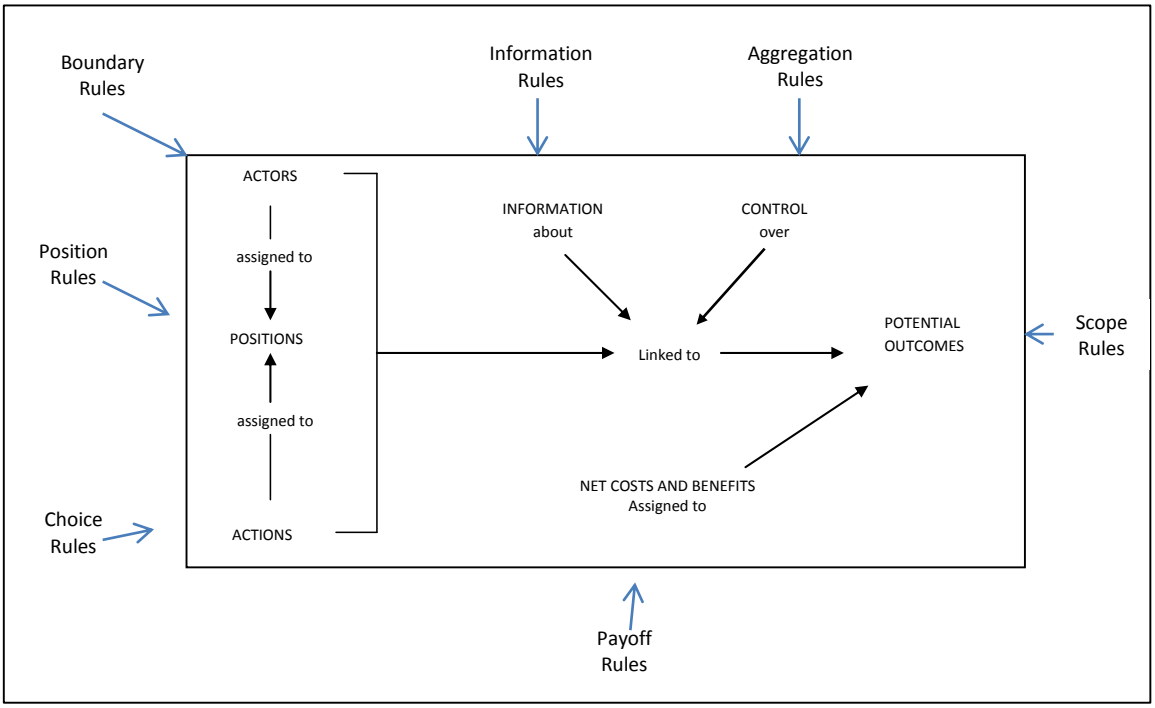

Figure 5-3 Rules Affecting Action Situation
Ostrom and Crawford, 2005

Rule configurations may describe “features” of a particular action situation. These features provide an indispensable instrument for diagnosing and/or modeling interactions that lead to specific outcomes (Aligica 2006, 89). Configurations of these rules have been suggested as a means of understanding policy change across time and organizations in a “rigorous manner” (E. Ostrom and Basurto 2011). However, Ostrom reminds us, the configuration of rule types alone is never “a necessary and sufficient explanation of the structure of an action situation and results” (E. Ostrom 2011, 19).

The IAD framework, as the Knapp model acknowledges, points to the effects of both the external and organizational conditions that describe the context within which an organization operates. The next section summarizes the external conditions for each case.

5.2 Discussion of External Standards

Several standards are referenced within the guidelines and procedures that constitute the USG Information Security Program. USG Security Awareness [Doc 403] specifically references Public Law 100-235 created the Computer System Security and Advisory Board and set in law a requirement that federal employees receive periodic, mandatory training [403:5]. Other references include Federal Information Processing Standards (FIPS) found in the Risk Management Policy [Doc 397]. The same document references the Risk Management Guide for Information Technology Systems (NIST SP 800-30) published by the National Institute of Standards and Technology. USG Security

Incident Management Policy [Doc 400] references the NIST Computer Security Incident Handling Guide (800-61). Outside of federal standards, the USG references ISO/IEC 27002:2005 as a process model for security policy.

I offer a discussion of these standards within the category of external conditions for two reasons. First, the adoption and implementation of a framework reflects the influence of external (peer and superior) networks on internal structures. Second, the individual case analysis revealed that management within each case treated these standards as external to the organizational structure and culture.

Two of the standards, the Association of College and University Administrators (ACUPA) model for policy development (ACUPA), and Agile, are process methodologies that are not specific to the creation of cybersecurity policy. ACUPA and Agile are models for governance of policy and are employed by the cases in that fashion. Payment Card Industry (PCI) standards, NIST, and ISO 27002 are standards that present both governance and policy standards for the cases to follow. These three standards may affect both the governance and policy structure for a case.

ACUPA provides specificity for the steps required to successfully add, delete or modify a policy on a campus. ACUPA defines steps within each major task. Adaptation of the ACUPA steps within the Knapp model provides an elegant means of breaking the analysis of institutions and actors into "buckets" of action small enough to aid analysis without losing sight of the big picture. The mapping of the major tasks with the Knapp model maintains consistency between my research model and the analysis found in the next two chapters. The ease of which the policy processes identified in each case map

into these steps is an indication of the positive and consistent influence on the structure of the case cybersecurity policy processes.

Agile is a design methodology that focuses on the inclusion of all stakeholders in a process that moves very quickly towards a consensus-driven set of outcomes. The "bottom-up" focus of the methodology resembles the standard for stakeholder inclusion found in the ISO standard that is also discussed. AGILE was explicitly identified in interviews with the Georgia Southern CIO as the model used to structure cybersecurity governance at the school.

PCI is specific towards protecting the integrity of the electronic payment systems managed by the credit card processing industry. Other than expecting a general information security policy, PCI is not concerned so much with the details of policy making as it is with the implementation and enforcement of practices to prevent the theft of credit card data. The role of PCI, as noted in the case descriptive summaries, is that of a catalyst causing a campus to review and restructure security governance with a payoff of mitigating or avoiding costly fines and loss of service.

Finally, the ISO standard is one that has influenced only Georgia State, even though the USG has endorsed the standard as an acceptable path. Nonetheless, implementation of ISO is voluntary and, as implemented by GSU, represents an effort by a campus to implement a standard that was not initially endorsed by USG staff. The NIST standard is referenced but not observed as affecting policy governance structure.

5.2.1 ACUPA

The University System of Georgia formally adopted, or at least suggested, the Association of College and University Administrators (ACUPA) model for policy development in 2009 (Figure 5-4) [23]. The USG instructions for policy and compliance management described three phases of policy development: Formulate, Refine, Formalize. Those three phases are echoed in the ACUPA standard as: Predevelopment, Development, and Maintenance. The ACUPA standard is uniformly supported by all 4 cases.

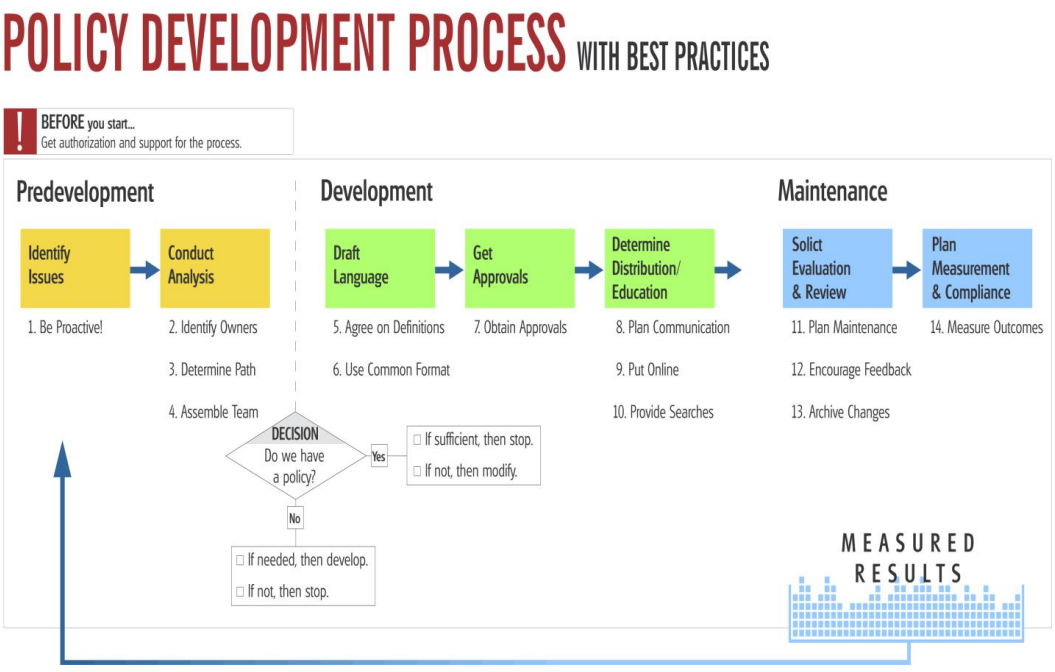

Figure 5-4 ACUPA Process Flow

The ACUPA model is a practical guide to link the observations as the cases studied relied on the ACUPA steps to inform their practices (Table 5-3). Basurto,

[23] *Found at http://www.usg.edu/infosec/policy_and_compliance_management last accessed 11 Apr 12*

Kingsley, et al., suggested that a researcher could sort their observations into "common sections and subsections that share the same broad aim" (2010a, 528). The ACUPA action steps provide a finer level of detail for the Knapp model as each step "nests" within a Knapp Process. The Knapp model reflects research specific to the processes required for effective cybersecurity governance. However, cybersecurity research is weak when it comes to describing the structural details of those required processes. Incorporating ACUPA into the research model provides an "anatomical guide" that describes the skeletal, muscular, respiratory, and other organs that should be present when examining the institutions and actors within the governance structure of each case.

How do the ACUPA "organs" relate to Knapp? Examination of the Actions within each ACUPA step reveals a set of verbs that denote the aIm component. The aIm component indicates the purpose or goal of the statement. The aIm verbs in Table 5-4 emphasize the creation, maintenance, documentation, and implementation of controls, standards, architecture, procedures and plans deemed sufficient by the USG unit to secure the "confidentiality, integrity, and availability" of USG information. The Conditions expressed in the observations emphasize a reliance on USG policies and standards to guide these actions. Taken together, these statements are meta-policies that define what each campus should do in order to comply with USG policy. The collection of Rule types within each step represent the rule configurations of the USG meta-policies.

Table 5-3 ACUPA Action Sets

ACUPA Situation	Step #	Actions	Knapp Action
1. Identify Issues	.01	Scans for changes in law, threat, best practices, organizational change, technology change, need to control risky behavior	Risk
	.02	may identify need/issue	Development
2. Conduct Analysis	.01	Identify Owners	Development
	.02	Determine Path (Policy Plan – Scope Definition)	Development
	.03	Assemble Team	Development
	.04	Gather Data	Development
	.05	Id deadlines	Development
	.06	Determine Risks	Risk
	.07	Determine Stakeholders	Development
	.08	Determine solutions for the problem/need	Development
	.09	Determine if present policy can be revised	Development
	.10	Determine need for new policy	Development
3. Draft Policy	.01	Agree on Definitions	Development
	.02	Drafts Policy -Use Common Format	Development
	.03	presents drafts to stakeholders	Development
	.04	review and vet proposals	Development
	.05	presents to policy advisory Committee	Development
4. Get Approvals	.01	Presents policies for approval to advisory committee	Approval
	.02	Considers/approves/modifies proposals	Approval
	.03	collects comments/revises as needed	Approval
	.04	Obtain Approvals	Approval
5. Education (Awareness)	.01	Plan Communications	Awareness
	.02	Put online	Awareness
	.03	Provide searches	Awareness
	.04	Communicates policy to appropriate audiences	Awareness
6. Plan Maintenance (Review/Risk Assessment)	.01	Versions new policy	Maintain
	.02	Archives old poicy	Retirement
	.03	Establishes schedule for review	Review
	.04	Determines review procedures	Review
	.05	solicits feedback	Review
	.06	Reviews risk and Cost	Risk
	.07	Recommends whether policy still needed	Review
7. Measurement & Compliance	.01	Measures/monitors outcomes	Monitor
	.02	Enforcement	Enforcement

Table 5-4 USG Metapolicies across ACUPA Action Sets

ACUPA Set	Rule Type	aIm	oBjective	Condition	Ref
1.02 ID Need	SS1	employ	prudent information security policies, standards, and practices	to minimize the risk to the confidentiality, integrity, and availability (CIA) of USG information.	9 : 6
2.01 ID Policy Owners	A1	[ensure]	information security controls	appropriate and auditable are in place	9 : 12
	CC1	develop and maintain	an information security organization and architecture	for support of information security across the USG and support of activities between institutions.	9 : 9
	CC2	develop	information security plans	using the same guidelines as referred to above	9 : 20
2.02 Strategy	CC1	create and maintain	an internal information security technology infrastructure	consisting of an information security organization and program that ensures the confidentiality, availability, and integrity of all USG information assets	9 : 7
	CC2	develop	an individualized information security plan	that is consistent with the guidelines provided by the USG Office of Information Security (OIS); consisting of a set of information security policies, standards, and guidelines	9 : 13
	CC3	document	procedures	in the individualized information security plan.	9 : 19
2.08 Solutions	IC1	maintain	information security implementation guidelines	that the USO, all USG institutions, and the GPLS should consider in the development of their individualized information security plans.	9 : 10
5.04 Communicate Policy	CC1	include	methods	for ensuring that information regarding the applicable laws, regulations, guidelines, and policies is distributed and readily available to its user community	9 : 16
	II1	make	USG's employees (full/part-time employees and contractors)	aware of their basic information security responsibilities through an awareness program	403 : 9
5.05 Training	CC1	ensure	each person	is trained to perform [roles and responsibilities]	403 : 4
6.00 Maintenance	CC1	maintain	an individualized information security plan	consisting of a set of information security policies, standards, and guidelines that is consistent with the guidelines provided by the USG Office of Information Security (OIS).	9 : 13.2
6.03 Review Schedule	II1	submit	information security plan	to the OIS for periodic review	9 : 14
7.01 Monitor	CC1	[develop]	procedures	for reporting of incidents to the USO in a timely manner	9 : 18
8 Implement	CC1	implement	an individualized information security plan	consisting of a set of information security policies, standards, and guidelines that is consistent with the guidelines provided by the USG Office of Information Security (OIS).	9 : 13.1

Legend: Rule Types: A – Aggregation; C – Choice; I – Information; S – Scope

5.2.2 Agile

Agile was developed as a framework for collaborative design and construction of information systems. The application of the AGILE framework to policy development is appropriate given the premise that policies are constructed of institutions and institutions are similar to coding instructions. AGILE values map easily to values identified in the IAD framework (Table 5-5).

Table 5-5 Comparison AGILE and IAD Values

Agile	IAD
Individuals and interactions over processes and tools	Interaction between and among the various levels of action shape the outcomes of implementing policies (vertical action levels). Ostrom emphasized the interaction of actors and rule sets on those outcomes as well (horizontal action levels)
Working software over comprehensive documentation	Policy change, policy effects, rule change (norm shifts) preferred over creation of formal rules that become paper tigers
Customer Collaboration over contract negotiation	Collaboration among all actors within a policy situations is seen as key to success in much IAD research
Responding to change over following a plan	Responding to changes of the bio-physical world – the action situation changes (a rule configuration may be identical, yet differences in the bio-physical events will create a different action situation as sets of actions / possible outcomes are limited by the bio-physical and material conditions Ostrom 2005, 22).

One can think of this model as an empowered bottom-up organization. The manifesto was developed by a group of developers who believed the "top-down" model of system design and development failed to acknowledge the need to meet the customers' needs and treated people as the least important asset on the team. The

values inherent in the manifesto emphasize organizational models based on people that collaborate and trust one another to deliver software that functions as needed.

The Agile process emphasizes a self-organizing team that includes both technicians and customers. Meetings are frequent (daily) to examine project progress. Progress towards the goal is incremental as the team delivers pieces of working software to the customer for approval and feedback. The incremental approach, combined with the iterative steps that include design, code, test, collect feedback, and repeat. A very simple translation of AGILE principles into policy process institutions is shown in Table 5-6.

Table 5-6 AGILE Institutions Mapped into ACUPA Action Steps

Action Set	Rule type	Manifesto Principle	Policy Process Adaptation
2.02	Choice	The best architectures, requirements, and designs emerge from self-organizing teams.	Team shall manage the process as the team decides.
2.07 3.04	Boundary, Choice	Business people and developers must work together daily throughout the project.	Stakeholders will include technical,. Management, and operational actors Team will collaborate with stakeholders.
2.09	Boundary	Build projects around motivated individuals. Give them the environment and support they need, and trust them to get the job done.	Policy Owners will engage stakeholders committed to sound policy development.
2.09	Choice	Simplicity--the art of maximizing the amount of work not done--is essential.	Team shall simplify policy to minimize effort required to comply.
3.03	Information Rule	The most efficient and effective method of conveying information to and within a development team is face-to-face conversation.	Team will exchange information in face-to-face meetings as much as possible
3.03	Scope	Our highest priority is to satisfy the customer through early and continuous delivery of valuable software.	Policy owners will satisfy the stakeholders through timely and continuous policy actions.
3.05	Payoff	Working software is the primary measure of progress.	Team will receive commendation for maintaining progress by delivery of working policies
3.05	Payoff	Continuous attention to technical excellence and good design enhances agility.	Team shall improve policy effectiveness by focusing on technical excellence and good design.
4.03	Choice	Welcome changing requirements, even late in development. Agile processes harness change for the customer's competitive advantage.	Policy Owners will accept stakeholder input anytime in the cycle.
4.03	Choice	Deliver working software frequently, from a couple of weeks to a couple of months, with a preference to the shorter timescale.	Team will deliver viable policy drafts frequently during the development process. Determines a timescale – a condition to the action of delivery policy drafts.
6.03	Choice, scope	At regular intervals, the team reflects on how to become more effective, then tunes and adjusts its behavior accordingly.	Team will review the Policy Process for effectiveness on a regular basis. Team will adjust process to improve effectiveness.

5.2.3 PCI

The Payment Card Industry (PCI) Data Security Standard is designed to ensure that credit-card transaction systems are managed "to protect consumer data"(Rowlingson and Winsborrow 2006). The standard contains no guidelines regarding how policy is constructed. However, it does contain a number of procedures and policies that must be contained in the organization's security policy and must be verified by an audit of the PCI auditors (Table 5-7). Failure to comply with PCI standards can lead to fines and withdrawal or limitation of credit card services (Rowlingson and Winsborrow 2006, 19).

PCI standards and controls are intended for a limited range of functions (i.e. credit card transactions). The controls are mostly technical in nature. Most of the actions are best practice oriented and found in other security standards and guidelines. Two controls are relevant to development of policy on campus: 1) Regularly test security systems and processes; and, 2) Maintain a policy that addresses information security.

Table 5-7 PCI Data Security Controls - Source Rowlingson and Winsborrow 2006)

Data Security Standard (DSS) Control Topic
Install and maintain firewall configuration to protect data
Do not use vendor-supplied defaults for system passwords and other security passwords
Protect stored data
Encrypt transmission of cardholder data and sensitive information across public networks
Use and regularly update anti-virus software
Develop and maintain secure systems and applications
Restrict access to data by business need to know
Assign a unique ID to each person with computer access
Restrict physical access to cardholder data
Track and Monitor all access to network resources and cardholder data
Regularly test security systems and processes
Maintain a policy that addresses information security

5.2.4 ISO 27002

ISO 27002 is a set of standards that provides “a code of practice for information security management and a process framework for information security governance” (Rowlingson and Winsborrow 2006, 17). If the organization successfully provides evidence that it has implemented all the elements of the standard, that organization may receive a certificate of compliance. The ISO standard specifies the policy process in stages entitled ‘Plan-Do-Check-Act’:

- Plan - establish a security policy and relevant procedures and controls' then prepare a statement of the scope of its application, justifying why the controls were selected and why others were not;
- Do -- implement the security policy and relevant procedures;
- Check -- assess and measure the process performance, and report the results to management;
- Act -- take appropriate corrective actions (Mikko Siponen and Willison 2009, 268)

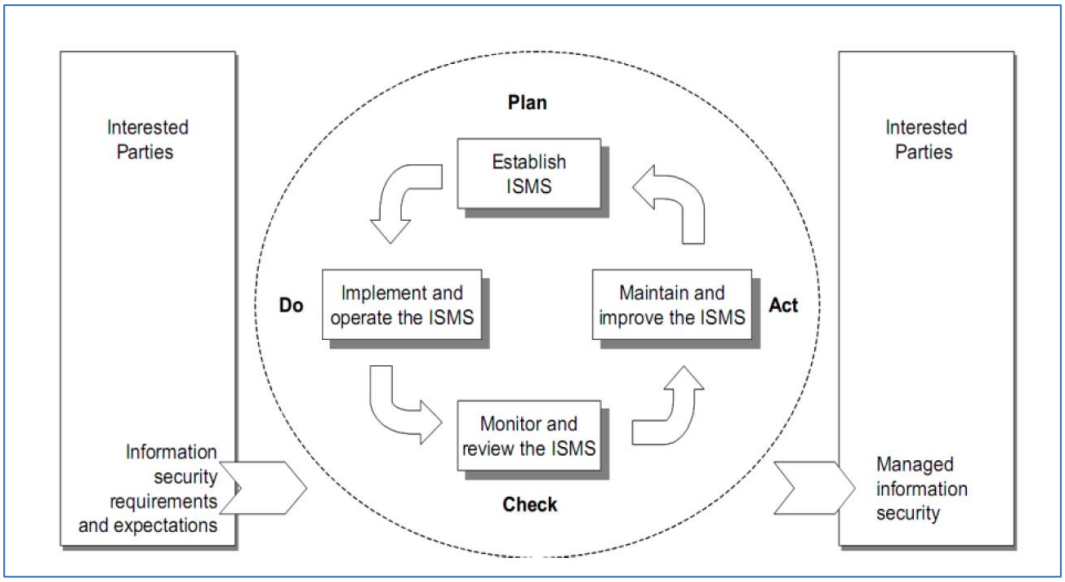

Figure 5-5 Plan-Do-Check-Act
(Siponen and Willison, 2009)

The main steps to develop an Information Security Management System (ISMS) are:

1. Obtain management approval for initiating an ISMS project
2. Define ISMS Scope, boundaries and ISMS policy
3. Conduct risk assessment and planning risk treatment
4. Conduct risk assessment and plan risk mitigation
5. Design the ISMS

(Asosheh, Hajinazari, and Khodkari 2013)

The structure of ISO27002 (Fig. 5-7) is similar to that of the Knapp structure. The Information Security Management System is equivalent to the ISO Governance. The security policy structure is composed of policies, standards, guidelines, procedures, plans and programs. The processes of risk assessment, monitoring (compliance), awareness (education), review (Maintenance), enforcement (response); are all present.

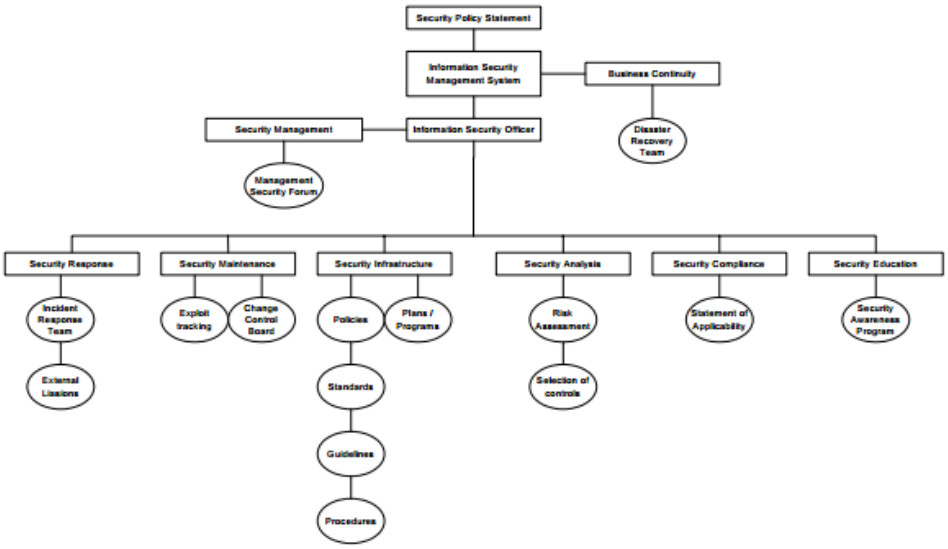

Figure 5-6 ISO 27002 Security Organization Structure

While the standard does not give guidance as to how policy should be written, it does specify details of what is expected (von Solms 2005). At the top level, there should be an overall "information security policy" that specifies how the policy aligns with organizational mission and objectives. The standard specifically sets expectations for top management of the organization to define "a set of policies to clarify their direction of, and support for, information security" (Karabacak and Sogukpinar 2006).

5.2.5 National Institute of Standards (NIST) Publication 800

The Federal Information Security Management Act (FISMA)[24] provides that the National Institute of Standards and Technology "prescribe standards and guidelines" to secure Federal information systems[25]. The executive order signed by Governor Perdue in 2008 referenced the NIST model for information technology security as a preferred, single model for all agencies of state government to follow. The effort to standardize on NIST was an effort to create a single view of security across state government and to ensure effectiveness of state security controls.

NIST defines a formal information security governance structure as:

> Information security governance can be defined as the process of establishing and maintaining a framework and supporting management structure and processes to provide assurance that information security strategies are aligned with and support business objectives, are consistent with applicable laws and regulations through adherence to policies and internal controls, and provide assignment of responsibility, all in an effort to manage risk.[26]

[24] Title III of the E-Government Act of 2002 (Pub. L. No. 107-347)

[25] Fiscal Year 2012 Report to Congress on the Implementation of the Federal Information Security Management Act of 2002" 2013, 1 - http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/fy12_fisma.pdf last accessed 26 Feb 2014

[26] Bowen, Pauline, Joan Hash, and Mark Wilson. 2006. "Information Security Handbook: A Guide for Managers". NIST Special Publication 800-100. Information Security. Gaithersburg MD: National Institute of Standards and Technology: US Department of Commerce. http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf.

The key activities that facilitate integrating information security governance activities with agency structure and activities are:

- strategic planning,
- organizational design and development,
- establishment of roles and responsibilities,
- integration with the enterprise architecture, and
- documentation of security objectives in policies and guidance[27].

The standard contains no guidelines regarding the policy process (how to develop the policy). The document details positions and responsibilities, but does not provide the structure to create policy as seen in ACUPA, ISO, and other standards. Beyond a reference here and there, there is no finding of influence on a case's governance structure.

5.3 Case Summaries

The study design employed "replication logic" to select cases where policy variations occur among "similar" organizations. Four research universities, University of Georgia, Georgia Tech, Georgia State, and Georgia Southern were selected. Descriptive meta-data are found in table 5-8. The organizational factors of interest, as set by the research model, include culture, size (population and resources available), and mission. I examine external threats and industry standards that apply to each unit as the external

[27] Ibid, p. 5

factors of interest for this study[28]. I discuss the findings of hypotheses related to the effects of internal and external conditions on the governance structure in chapter 6. The evidence presented here should be read as a "prologue" for that discussion.

Table 5-8 Case Descriptive Data

Factor	**Georgia Tech (GT)**	**Georgia Southern (GS)**	**Univ. of Georgia (UGA)**	**Georgia State (GSU)**
Size (Students enrolled)	19,431	19,150	33,367	30,606
Carnegie Class	RU/VH, DR	DRU, DR	RU/VH, DR	RU/VH, DR
Security Office	ISO – one person focused on security, additional personnel focused on compliance, monitoring, implementation	ISO one person, other responsibilities	ISO – one person focused on security, responsibilities for implementation and monitoring distributed across the organization	ISO –two persons, security officer and security engineer
External				
Industry Standards	ACUPA, PCI	ACUPA, PCI, Agile	ACUPA, PCI, ISO 31000	ACUPA, ISO 27001/31000
External Threats	Credit Card Breach	Credit Card Breach	Credit Card Breach	None Reported

For each case, observations of institutions tagged for an ACUPA step are counted (Table 5-9). I cover the configuration of rules for each case and step in Chapter 6[29]. However, this "x-ray" of the structure for each case suggests some structures may be relatively stronger than others.

[28] The limitation is due mostly to resources (time and human capital). I also find defense in Ostrom's standard that as we analyze an action situation, we hold the exogenous conditions constant (2005). The external threats are observed to vary for each case and are therefore included.

[29] If the reader wishes, the institutions are presented in tables found in the Appendix sorted by ACUPA Step. GSU – Appendix I. GS – Appendix J. GT – Appendix K. UGA – Appendix L.

Table 5-9 Summary Data - Distribution of Meta-policy observations

ACUPA Situation		Step	Actions	Cases				
				Ga Sou	GSU	GT	UGA	Sum
1. Identify Issues		1.01	Scans for changes in law, threat, best practices, organizational change, technology change, need to control risky behavior	0	2	1	0	3
		1.02	may identify need/issue	1	1	0	0	2
		2.00	Miscellaneous	0	0	1	0	1
2. Conduct Analysis		2.01	Identify Owners	4	2	3	1	10
		2.02	Determine Path (Policy Plan – Scope Definition)	2	0	1	3	6
		2.03	Assemble Team	3	3	8	15	29
		2.04	Gather Data	1	0	0	2	3
		2.05	Id deadlines	0	0	0	0	0
		2.06	Determine Risks	1	2	0	1	4
		2.07	Determine Stakeholders	3	0	1	3	7
		2.08	Determine solutions for the problem/need	0	1	2	0	3
		2.09	Determine if present policy can be revised	3	2	1	1	7
		2.10	Determine need for new policy	2	1	0	2	5
3. Draft Policy		3.01	Agree on Definitions	1	0	0	0	1
		3.02	Drafts Policy -Use Common Format	4	4	2	0	10
		3.03	presents drafts to stakeholders	5	3	2	1	11
		3.04	review and vet proposals	1	1	5	2	9
		3.05	presents to policy advisory Committee	1	0	3	0	4
4. Get Approvals		4.01	Presents policies for approval to advisory committee	2	6	1	0	9
		4.02	Considers/approves/modifies proposals	0	13	3	0	16
		4.03	collects comments/revises as needed	6	4	5	0	15
		4.04	Obtain Approvals	1	4	0	5	10
5. Education (Awareness)		5.01	Plan Communications	2	0	0	1	3
		5.02	Put online	1	2	2	0	5
		5.03	Provide searches	1	0	0	0	1
		5.04	Communicates policy to audiences	3	3	3	0	9
6. Plan Maintenance (Review/Risk Assessment)		6.01	Versions new policy	1	7	2	0	10
		6.02	Archives old policy	3	0	0	0	3
		6.03	Establishes schedule for review	1	1	2	2	6
		6.04	Determines review procedures	4	9	3	8	24
		6.05	solicits feedback	0	0	4	3	7
		6.06	Reviews risk and Cost	4	0	8	0	12
		6.07	Recommends whether policy still needed	4	0	1	0	5
		7.00	Miscellaneous	0	0	1	0	1
7. Measurement & Compliance		7.01	Measures/monitors outcomes	0	5	0	1	6
		7.02	Enforcement	0	0	0	4	4
Sum				65	76	65	55	261

5.3.1 Georgia Tech

Georgia Tech approved a meta-policy that defined cybersecurity policy governance in 2008 (Document 360 - "*Policy Review Process")*. Two other documents, "*Information Security Exception Policy" [353],* and *"Policy Exception Procedures" [359],* followed. The policies and procedures[30] for "exceptions" to university policy recognized a need to tailor and/or change the scope of some policy due to differences in organizational factors at the sub-unit level (i.e. Georgia Tech Research Institute, School of Computer Science, etc.). The meta-policy follows the ACUPA model, with some influence from the PCI (Payment Card Industry) model in areas that interface with credit card data[31]. Interview data indicates the campus policy structure is influenced by the ISO standards and federal cybersecurity standards.

Prior to 2008, Georgia Tech's security governance was an accurate reflection of the "loosely coupled" description. College, department, and auxiliary units could supplement and supersede policies created at university level. Compliance to a university-wide policy was not enforced. As a result, policies differed among the colleges and departments of the university.

A couple of high-profile incidents motivated the President of Georgia Tech to change that structure. A breach of a server housed at the campus theatre reaped

[30] The observations found in the "*Procedures*" document are coded as metapolicy statements as the statements manage the exception requests from departments as though the requests are amendments to the policy – therefore these instructions focus on how to create/amend/delete policy which is the definition of a metapolicy statement.

[31] PCI representatives required formal policies to protect against future thefts of credit card data after the Ferst incident.

thousands of credit card numbers including those of President Jimmy Carter, Ambassador Andrew Young, and many notable CEO's in the Atlanta Area. The breach occurred because the theatre failed to install software patches regularly as required by university policy.

Within a year, an email server maintained by the College of Biochemistry was hacked. The server began to congest the university network with denial-of-service attacks. The dean of the college rejected offers from the university Office of Information Technology to help, saying, "We have smart people, we can handle the incident ourselves." The OIT had no choice but to physically disconnect the college from the university network. After several months of "downtime" for the college's email server, the college was able to restore mail services.

The GT President issued instructions to the university vice presidents and the college deans that any future breaches of security found to occur because of non-compliance would not be tolerated. At this time, the university's deep cultural ties to autonomy were re-examined.

Under the new governance structure, "Campus units are allowed to have their own policies, but they can't supersede institution policy."[32] Document 359 reflects the Georgia Tech culture as it values autonomy. The structure is also an acknowledgement that differing local context requires a tailoring of policy to make policy effective.

However, compliance among GT units does vary. USG policy and Georgia Tech policy require business continuity and disaster recovery plans, but compliance is not

[32] Lummis, Jimmy (Policy Compliance Manager). (22 March 2012) Telephone interview.

strictly enforced. The Chief Information Security Office of Georgia Tech explains how they manage what is an issue of compliance with USG policy:

> *"…because the centralized organization does not control the budgets within the departments, we put in the policy some business continuity kind of statements and then the procedures and guidelines to follow. And, basically we leave it up to the units to determine how much infrastructure they want to maintain locally. If you decide to maintain local infrastructure, then you have to include business continuity and our internal auditors do audit for that. So, they get to determine their threshold when it comes to infrastructure continuity. We just set the top level policy and what continuity should look like."*[33]

5.3.2 UGA

UGA experienced more than one significant breach of stored credit card data in 2004-2005. Auditors from the Payment Card Industry (PCI) insisted on major changes in the policies that governed data security. Like Georgia Tech, the Office of the President engaged in the process, as well as the Office of the Provost. Concurrent with the Governor's executive order of 2008, the Provost of the University of Georgia issued a memo denoting the responsibility of everyone at UGA to follow the new security guidelines. Unlike Georgia Tech, UGA did not formalize a policy review and exception process with a metapolicy.

UGA responded to the incident with the Credit Card Policy [380], and a plan entitled SecureGA [466]. UGA followed the ACUPA policy management scheme. In addition, the university's *Credit Card Processing* policy indicates that standards from ISO 17799[34] and the Payment Card Industry (PCI) standards contributed to the security

[33] Baines, Herb. (22 March 2012) Telephone interview.

[34] International Standards Organization document defining computer standards. This document was superseded by ISO 27002:2005 just a few months after its publication. ISO 27002:2005 "establishes

program [380:2]. In addition, the role-based accountability model discussed in the SecureGA plan [466] relied upon National Institute of Standards and Technology (NIST) publication 800-16, "Information Technology Security Training Requirements: A Role- and Performance-based Model." In sum, all the standards for creating security policy were referenced.

However, these mandates did not precede the creation of a formal metapolicy as was the case for GT. At UGA, if a policy is required by an external organization, UGA will not develop policy documents that may replicate the mandated policy. I asked the UGA CISO: "When you have a requirement sourced from an external source, such as the Board of Regents or the Payment Card Industry (PCI), do you respond in an ad hoc fashion?"

> *CISO: Certainly. Now usually what we tend to do, as opposed to regurgitate what it is in a law in our policy, we'll take more of an awareness stance. There are a couple of sites that we have that explains what our requirements are as opposed to just having a specific incident handling policies for instance. We have a website that says what you can and cannot do with this based on these legal references. And that we've found is a lot easier to socialize and enforce and a lot easier to get out in the public's hands quickly. [post 30:32]*

guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization" – found at http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=50297. Last accessed 29 Dec 2014.

Interviewer: So guidelines and standards are accepted more easily than law or policy?

CISO: No, what I'm saying is that I think law is a lot harder to argue with. So what we've essentially done is in a lot of these cases. HIPPA is another case. We will explain what that the requirements on the UGA are under the law and make that available to them and a part of the training. Beyond that what's created next is a central set of procedures that enable us to comply with those laws. And we do the same with USG policies. We don't have an incident management policy because USG has one. We have a reference and explanation of incident management at USG and then an explanation of how UGA handles those procedures to comply with those policies.

This practice of referencing members of the UGA organization to external policies is unique among the four cases. Policy owners develop guidelines and awareness activities to inform stakeholders of the external requirements. Policy owners place references to these external requirements. UGA's structure reflects a heterogeneous network of inter- and intra-organizational policy documents.

In general, the university policy will establish responsibility of what needs to be done. Departments may determine how to comply with policy in some cases. The university may distribute authority to enforce compliance with policies to departments, offices, colleges and other sub-units of the university. A student who misuses an asset may be prosecuted under the student conduct code. A faculty member may find

themselves subject to discipline by their college. A staff member may be disciplined by the Human Resources department.

The responsibility for implementing, monitoring, and enforcing these standards is left to the individual departments, divisions, and other units. Activities at the collective level for policy development, under this model, are minimal with the output constrained to a reference to the externally required mandate. Awareness activities are decentralized as the units are responsible for making users aware. Operational level activities are entirely decentralized.

The data indicates a high cost for engaging a centralized policy process to develop or modify policy. The process for gaining support to adopt new or revised policies may take up to 2 years. Referencing external policies is seen as a means of complying while avoiding costly and time-consuming drafting and approval processes.

5.3.3 Georgia Southern

The CIO of Georgia Southern acknowledged that proposing and adopting new policies "…can take years to debate, if you're not careful"[35]. The CIO noted that universities are delegated authority to "…establish policy and procedures which suit our particular environment." However, "we get into a lot of trouble legal-wise when we have a policy that we do not follow or a policy that is followed inconsistently". Such inconsistency requires central policy, monitoring, and review.

[35] Burrell, Dr. Steven. (13 April 2012). Telephone interview.

The CIO cited a "pre-audit" visit as one factor prompting the revision of the Acceptable Use Policy at Georgia Southern. A "pre-audit" visit is a meeting that involves the audit team leaders and the campus committee responsible for assisting the audit team. The audit team will discuss the areas to be audited and ask the campus team to prepare for the audit by identifying and organizing relevant documents that will be needed by the team to complete the audit. This particular visit discussed the audit team's intent to review information security policies. The GS IT team reviewed the Acceptable Use Policy and the Copyright provisions of the Higher Education Opportunity Act policy and modified them as needed to position the university to defend its reputation for compliance to law and policy.

The CIO adopted a method created by software developers to improve the quality and responsiveness of programmers to customer requests. The AGILE process emphasizes a self-organizing team that includes both technicians and customers[36]. Georgia Southern modified the AGILE Development Process to guide the development of IT policy. AGILE principles promote collaboration with stakeholders as a priority. The AGILE process is a "bottom-up" approach focused on rapid, incremental progress towards development of systems for the organization. The emphasis of the process is creation of "working policy" rather than development of a carefully worded policy document. The application of AGILE principles to the Georgia Southern policy structure

[36] The principles of AGILE development are found in a manifesto http://agilemanifesto.org/principles.html.

provides a comparatively rapid policy development cycle (4-6 months) as compared to UGA or Georgia State (1 – 2 years).

Followers of Agile principles value the ability to respond to change versus how well a formal plan is followed. Emergent organizations depend upon the flexibility offered by such principles. Dr. Burrell described how those principles drove the frequency and scope of interaction between and among the IT personnel responsible for developing policy and the stakeholders affected by the policy change.

> *"… using the AGILE process, getting immediate feedback, starting from some place. If you give people a blank page, they don't know where to start. So it's easier to give them something to criticize than it is to ask them to come up with something original. And I don't mind people criticizing my writing….and then give them immediate feedback…..24 to 48 hour period to turn that document back around for consideration. A lot of that can be done through email correspondence once you've laid it all out there for them. And then troll that to the next group and so on. During the interview process you end up with some ends to it and then you troll it back by high level managers, taking a slightly different slice, taking a functional slice and that process has worked pretty well for us here." Dr. Steven Burrell*

Like UGA and Georgia Tech, Georgia Southern experienced a data breach in 2006 that compromised the bookstore financial system. This incident involved merchant banks and required a repair to the integrity of the organization's financial systems. The event raised awareness of security protocols within the university. General media news reports may have helped to construct a norm that is important to the organizational culture:

> *"I just think the media has helped us in some respects that the issues of computer hackers and bad things happening to good people out there has become more a part of daily consciousness of people by virtue of media news and richness of all that."*

It is important to recognize how the AGILE development philosophy is reflected within the organizational culture and norms related to university policy development. The CIO of Georgia Southern describes a collegial environment where Vice Presidents and their delegates work across the functional areas of the university to develop policy. Strong top management support of adopted policies is an outcome of that environment.

As to the "security culture", the CIO believes the employees and students at Georgia Southern have accepted the idea that "security is just as much their responsibility as somebody else's". He attributes this understanding as one reason why he does not see systematic resistance when security policies are added/changed and implemented.

The "understanding" among the stakeholders is an expected consequence of the "bottom-up" approach to policy achieved through implementation of the AGILE methodology. Collaboration, an organizational condition necessary for effective policy, is a key value. Collaboration is emphasized in the principles of AGILE. For example, consensus of the team is an expected Aggregate rule under AGILE. Other understand rules and norms include:

- Engagement of all stakeholders
- Free exchange of information
- Continuous and timely discussions
- And others (See Table 5-6).

GS security policies were developed following a process formalized as a document [336] in 2010 entitled "*IT Policy Development and Review Process".*

Whenever an initial assessment determined that a policy addition or revision was required, a network of committees was engaged that included Vice Presidents as chairs and co-chairs. Those committees would examine the policy changes in the context of the committee constituencies (deans, students, business managers, etc.). The Georgia Southern policy process follows the outline suggested by the ACUPA model. The AGILE principles, in concert with the University process for approving and implementing IT policy [336], provide the detail needed to identify the governance structure.

The CIO of Georgia Southern stressed the distinction between university policy and the procedures and guidelines used by a department or division:

> *A University policy is an official statement expressing the position of the University on an issue of institution-wide importance. A policy guides the decisions and actions of the institution and is consistent with its mission. As such, it meets the following criteria:*
>
> - *The administrative authority of the University or the Board of Regents of the University System of Georgia has sanctioned it.*
> - *It has a broad institution-wide application.*
> - *It is a governing principle for both established and future activities of the University.*
> - *It exists to ensure consistency in University practice to conform to the University's mission and goals, Federal and State legislation, and other legal requirements.*
>
> *If a policy fits these criteria, it is a University policy. If it does not, it is a departmental, office or unit policy or guideline. No collection of policies and procedures can anticipate every circumstance. The contents of these policies are subject to change from time to time. As policies and procedures change, the University will make necessary revisions*
>
> *("Georgia Southern University Policies" 2013)*

Procedures and guidelines handled at the department level are not elevated for cabinet approval. Departmental procedures and guidelines may manage the

implementation of policy but cannot substantively change policy, another distinction emphasized by Dr. Burrell in the interview.

> *"There may be some different procedures that are followed in various department or what not but I don't call those policy changes." –Dr. Burrell (Interview by author).*

The collective level process resembles the GT process in the following ways: 1) Includes all top management; 2) includes all stakeholders in the decision chain; and 3) emphasizes flow of information. However the Policy Process document [336] is not as formal with regards to positions, responsibilities, and tasks as the GT metapolicy. The GS process, as stated earlier, restates the ACUPA model with minimum specificity regarding the GS organizational structure. In other words, "tailoring" of the process is minimal. However, the adoption of the AGILE methodology introduced a number of norms into the GS process that are similar to the GT rules. The process may be less formal, but the cost of outcomes, measured in terms of time and resources to modify or create policy are very similar.

5.3.4 GSU

GSU has experienced no significant breach of security in the time period covered. The lack of external threats manifested as breaches in security or thefts of confidential data certainly contrasts with that of the other three cases.

The structure of the policy process encases a network of action situations. My interview of the CISO at GSU confirmed that the university employs formal and informal institutions to govern the policy process. Two different policy models manage the policy process. The ACUPA model is represented by the university policy on university policies.

The policy explains how university-wide policies are to be developed, approved, and managed. However, this process is not binding on "policies developed by individual colleges, schools, divisions, or departments to govern their internal operations"[37] The CISO led an effort to implement the ISO 27002 process model but only two areas achieved certification, financial systems and the data center. The lack of financial resources as allocated by the university governance process prevented certifying other areas of the university. The influence of ISO 27002, as a meta-policy, is limited to the scope of the Information Security Management System Policy (Document 367).

The Office of Legal Affairs constrains the agenda and scope according to their interpretation of need and risk. The Office of Legal Affairs decides whether the need identified requires a new policy, a modification of existing policy, or no action. This office acts as the guardian of policy for the university and maintains a central catalog of university policies and procedures. The office must accept the CISO's argument that the need for policy is significant and that the objectives cannot be achieved by an existing policy. The university attempts to create "umbrella" policies that are broad in scope, yet flexible in application, to minimize creation of a number of "specialty" policies.

The CISO stated that as she tried to push for compliance with Payment Card Industry (PCI) requirements, the Office of Legal Affairs noted the requirements were not law. The office did not believe the risk of a breach of financial systems employing

[37] Procedural Guidelines on University Policy on University-Wide Polices. Found at https://app.gsu.edu/policies/search_policies.cfm?view_policy=4924. Last accessed 29 Mar 2014.

credit/debit cards was high. The adoption of the PCI standards to secure credit card transactions was deferred due to cost and a perception of low risk.

The narrative discusses two examples of the effects of autonomy. The University-Wide Policy on Policies explicitly defers to sub-units to determine their individual governance structure. Guidelines employed by the Office of Legal Affairs defend existing policy as preferable to adaptation of external requirements. It is a mistake to characterize the policy structure as "decentralized". Departments and divisions do exercise certain levels of autonomy in making policy specific to their units. However, when a department wishes to implement a "department-only" policy that requires university resources to implement, the request for those resources travels through a centralized procedure for analysis of risk and budget capacity.

The cost of modifying or creating policy, measured in terms of time and resources, are similar to that of UGA, 18-24 months. The absence of a significant breach at GSU suggests a low risk to not modifying policy. The CISO did not share in the perception of "low-risk", but, the decision of the Office of Legal Affairs seems justified by their perception of risk. Similarly, the CISO was unable to expand implementation of the ISO 27001 standard due to a difference in the perception of risk and the significant cost for implementing the standard.

5.4 Summary

I have summarized four standards that are identified by the cases as influential on the structure of the information security policies each has adopted. As the Knapp

model reflects the standards implemented by practitioners across the industry, it is no surprise that this summary confirms the each of the four standards is sympathetic with the Knapp model.

These standards are the most significant influences of the external conditions identified in this study, as confirmed by interviews with officials responsible for constructing security policy. An initial scan of the structure of each case per the ACUPA steps indicates substantial variation among the cases. The case summaries indicate reasons given for the different configurations shown in each case. The next chapter will summarize notable organizational conditions and the policy governance structures for each case. Analysis in the next chapter will highlight institutions selected from the external mandates and standards. The IAD descriptors will reveal differences in governance due to the selections among the cases by examining the variation in the attributes, aims and conditions that determine actors and institutions in use.

Chapter 6- Governance Structures

The Knapp model summarizes the theoretical and practical consensus of an ideal structure of cybersecurity governance. Details as to the structure of the individual policy processes is an admitted weak point of the information security literature. The previous chapter noted a number of standards, in particular ACUPA, as those standards can be applied within the Knapp model. All of the standards that have been discussed emphasize a governance structure that engages all stakeholders in a manner that aligns policy with organizational goals while maintaining an appropriate fit between the policy objectives and the context of the organizational condition. These definitions serve as a baseline from which I can identify elements of policy structure that may contribute to determining the structure of policy produced.

The central hypothesis suggests that effective cybersecurity policy and management practices are preceded by an effective governance structure. Governance structure is measured along a continuum from ad hoc, with few but not all of the necessary processes, components and conditions, to formal, with a formal metapolicy and all of the Knapp processes and appropriate policy components. Effective policy becomes more likely as the governance structure approaches a formal status.

I borrow the IAD's definition of structure as the configuration of actors and rules that constrain the actors' choices that lead to outcomes. The IAD framework and the Knapp model both suggest that variations in governance structure are related to variations in external and organizational conditions. Mapping the ACUPA steps into the

Knapp model adds needed precision to measure differences in governance and policy structure as they relate to variation of select internal and external conditions

This study focuses on three of those conditions: external policy standards, organizational top management support, and organizational collaboration. The effects of those conditions are expected to influence the structure of the governance for each case. Those variations in structure are expected to be manifested by variations in the structure of policy produced for each case.

The findings are presented as observations of varying configurations of institutions (rules) and actors that describe the security policy for each case. The rule configurations represent an aggregation of statements collected from Policy Documents[38] as units of observation. These observations are aggregated to draw conclusions on organizational structure (the cases are the units of analysis)[39]. Observations are nested by major ACUPA task and are presented in Appendices M through Q. Analysis of observations focused on the components aIm (I), oBject (B), and Condition (C).

The research model is built upon information security research that finds effective cybersecurity is preceded by effective policy and effective management practices to implement that policy. The qualities of both policy and management practices are preceded by the quality of the policy processes, the governance structure that defines the policy and the environment to support effective management

[38] See Appendix I for list of documents per case that contributed to the data analyzed.
[39] See Basurto, et al. 2010 for more discussion on aggregating units of observations for the units of analyses.

practices. Policy structure reflects governance structure. The success of the former depends heavily upon the latter.

In the analysis that follows, I reference noted observations through the use of square brackets []. Within the brackets, I identify the document [Doc ID] and the observation [:obs id]. For example, the second observation [:2] from the interview of the UGA CISO [471] would be referenced as [471:2].

This chapter starts with an examination of the governance structure. I begin with a rudimentary analysis of case descriptive data and case policy documents building upon the research cited in chapters 2 and 3. That analysis is joined with analysis of structure as prescribed by the IAD framework. The second section presents findings regarding key features of governance structure influenced by Top Management Support, Collaboration, and the external policy standard that influenced each case. The third section compares policy structures for each case and the respective relationships with governance structure. A summary of these findings closes the chapter.

6.1 Comparing Structures – Preliminary Analysis

H1: The structure of a policy governance process will be reflected in the formality of the policy structure created by that process.

My first hypothesis explores the relationship between formal policy processes and policy structure. If a university has a formal meta-policy, then I expect to find a more formal policy structure, one that presents more policy components (policies,

procedures) within a policy area and one that connect policy areas (data protection, privacy) by sharing components such as guidelines and procedures. Such sharing is indicated by documents referencing each other. The sharing of components indicates a plan to efficiently along organizational resources with policy objectives. Various components, such as procedures and guidelines, are used to "fit" the policy within sub-units of the organization that must tailor the policy to unique needs or conditions. The lack of components, and more importantly, the lack of documented policy, is noted as a condition that signals the lack of organizational resolve to managing the policy problem (Knapp and Ferrante 2014, 2009).

6.1.1 Document Level Analysis

The first test of hypothesis number one examines whether a document structure, as proposed by Doherty, et al (2009), and the process structure proposed by Knapp, et al (2009) show increasing formality when comparing universities with and without meta-policies. Georgia Tech and Georgia Southern have formal meta-policies. UGA and Georgia State have similar documents, but neither are in-use on a university wide bases. All four have observations that are coded as meta-policy statements. These aggregations represent an informal metapolicy.

So, to begin, each case was examined and data gathered to answer the three questions found in the Doherty paper (2009):

1) Policies cover how many security issues?
2) How many documents compose the policy?
3) How do the documents relate to each other?

The data found in Table 6-1 speak to the first two questions.

Table 6-1 Case Policy Descriptive Statistics

Legend
N
Chi-square contribution

N / Row Total
N / Col Total
N / Table Total

Pearson's Chi-squared test

Chi^2 = 742.9476 d.f. = 39 p = 6.221765e-131

Policy Area	UGA (11)	Ga Southern (11)	GSU (17)	GT (7)	Row Total
AUP	107	117	92	145	461
	3.35	0.11	5.34	17.29	
	0.23	0.25	0.20	0.31	0.29
	0.24	0.30	0.23	0.41	
	0.07	0.07	0.06	0.09	
---	---	---	---	---	---
Awareness	25	4	0	3	32
	29.39	1.91	8.12	2.40	
	0.78	0.12	0.00	0.09	0.02
	0.06	0.01	0.00	0.01	
	0.02	0.00	0.00	0.00	
---	---	---	---	---	---
Copyright	5	27	8	5	45
	4.47	22.87	1.02	2.53	
	0.11	0.60	0.18	0.11	0.03
	0.01	0.07	0.02	0.01	
	0.00	0.02	0.01	0.00	
---	---	---	---	---	---
Data Handling	52	73	13	105	243
	3.48	2.90	38.40	47.61	
	0.21	0.30	0.05	0.43	0.15
	0.12	0.19	0.03	0.29	
	0.03	0.05	0.01	0.07	
---	---	---	---	---	---
Incident	3	37	12	0	52
	9.03	45.72	0.11	11.60	
	0.06	0.71	0.23	0.00	0.03
	0.01	0.09	0.03	0.00	
	0.00	0.02	0.01	0.00	
---	---	---	---	---	---
Information Security Program	157	86	154	93	490
	3.34	9.96	7.07	2.43	
	0.32	0.18	0.31	0.19	0.31
	0.36	0.22	0.38	0.26	
	0.10	0.05	0.10	0.06	
---	---	---	---	---	---

Table 6-1 (continued)

Policy Area	UGA (11)	Ga Southern (11)	GSU (17)	GT (7)	Row Total
Password	32	0	0	1	33
	57.19	8.13	8.37	5.50	
	0.97	0.00	0.00	0.03	0.02
	0.07	0.00	0.00	0.00	
	0.02	0.00	0.00	0.00	
---	---	---	---	---	---
Privacy	60	1	6	3	70
	85.09	15.29	7.79	10.19	
	0.86	0.01	0.09	0.04	0.04
	0.14	0.00	0.01	0.01	
	0.04	0.00	0.00	0.00	
---	---	---	---	---	---
HIPAA	1	0	0	0	1
	1.89	0.25	0.25	0.22	
	1.00	0.00	0.00	0.00	0.00
	0.00	0.00	0.00	0.00	
	0.00	0.00	0.00	0.00	
---	---	---	---	---	---
Continuity	0	1	0	1	2
	0.55	0.52	0.51	0.69	
	0.00	0.50	0.00	0.50	0.00
	0.00	0.00	0.00	0.00	
	0.00	0.00	0.00	0.00	
---	---	---	---	---	---
Cryptography	0	1	2	0	3
	0.83	0.09	2.02	0.67	
	0.00	0.33	0.67	0.00	0.00
	0.00	0.00	0.00	0.00	
	0.00	0.00	0.00	0.00	
---	---	---	---	---	---
Electronic Data Disposal	0	10	2	0	12
	3.32	16.80	0.36	2.68	
	0.00	0.83	0.17	0.00	0.01
	0.00	0.03	0.00	0.00	
	0.00	0.01	0.00	0.00	
---	---	---	---	---	---
Resource Management	0	36	112	0	148
	40.99	0.01	147.56	33.01	
	0.00	0.24	0.76	0.00	0.09
	0.00	0.09	0.28	0.00	
	0.00	0.02	0.07	0.00	
---	---	---	---	---	---

Table 6-1 (continued)

Policy Area	UGA (11)	Ga Southern (11)	GSU (17)	GT (7)	Row Total
Risk Mgt	0	0	4	0	4
	1.11	0.98	8.78	0.89	
	0.00	0.00	1.00	0.00	0.00
	0.00	0.00	0.01	0.00	
	0.00	0.00	0.00	0.00	
----------	----------	----------	----------	----------	----------
Column Total	442	393	405	356	1596
	0.28	0.25	0.25	0.22	
----------	----------	----------	----------	----------	----------

The policy issues on the left hand column represent issues the University System of Georgia (USG) requires each of its campuses to cover in their policy. The number underneath the case initials represents the number of documents that cover those issues for each case. The counts within the table represent the units of observation, statements, found within those documents as they align with the policy issue those statements are designed to regulate.

The table shows that among all cases, some issues receive more attention. Coverage of an Information Security Program and Acceptable Use Policies (AUP) represents 60 percent of all statements counted among the cases. Coverage for Risk Management, HIPAA (confidentiality of health data), Continuity planning, Cryptography, and Electronic Data Disposal receive almost no attention, comparatively. AUP is among the oldest of policy areas which may explain why so many issues are covered in one document. Areas such as continuity planning require greater inter-organizational collaboration and additional resources to plan and to test plans that will ensure the ability of an organization to continue to operate if security is compromised.

The literature suggests that well-structured policy consists of a variety of policy components (Table 6-2). Analysis of a policy document[40] identified individual statements that are categorized as the criteria in Table 6-1 suggest. The criteria for categorization used for analysis is found in appendix H.4. For this study, statements that did not meet the existing criteria and that referenced external documents were considered "Ancillary" components. Ancillary statements play an important role in connecting features of policy found across documents. So, these statements were not discarded.

Table 6-2 - Policy Components

Component (Legend)	Literature	USG
Meta Policy (Sphere)	Establishes how info sec policies are created, implemented, enforced (Baskerville & Siponen 2002)	Not mentioned
Policy (Solid Square)	management's requirements at a high level, defining "what is required" not "how to do it".(Moule & Giavara) Expresses concerns/objectives at "highest level of abstraction" (Baskerville and Siponen, 2002)	a concise document that outlines specific requirements, business rules or company stance that must be met. The policy is the organization's stance on an issue, program or system. It is a rule that everyone must meet.
Standard (Square)	Established rules or requirements that must be observed in the execution of procedures. (Baskerville and Siponen 2002)	a requirement that supports a policy Standards: Define minimum requirements designed to address certain risks Define specific requirements that ensure compliance with policies
Procedure (Solid Diamond)	instructions which must be followed in order to comply with prescribed policies and practices. (Moule & Giavara)	(N/A)
Guideline (Diamond)	suggestion, approach or issue that the reader should keep in mind when performing a particular task or activity (Moule & Giavara)	a document that suggests a path or guidance on how to achieve or reach compliance with a policy.
Ancillary Policies (Triangle)		Organizational policies referenced for enforcement or credibility reasons

[40] I found such a collection of components within some "policy documents" that the "document" was merely a container in which all sorts of statements are found. The documents for this study contained a range of policy areas and components. A collection of such containers bring to mind the "garbage can" that Cohen, March and Olsen (1972) used to describe the policy process found at many universities.

A graphical representation of the structure of policy components constructed by capturing references among policy documents for each case suggests some differences in policy structure. Georgia Tech (Figure 6-1) references almost all security policy documents from one information security document, the GT Computer and Network Usage and Security Policy [343]. The document references procedures (solid diamonds), policies (solid squares), guidelines (hollow diamond), and ancillary policies. The best formed structure is created by the process to review, develop, and approve policies. In the upper right hand corner of the graph, the sphere represents the document entitled "Policy Review Process" [360]. The document, a formal meta-policy, references an exception policy and procedures a unit of Georgia Tech must follow to request an exemption from a university-wide security policy. The arrows indicate the directional nature of the references found within each of those documents. Each individual document references the central information security policy [343] individually. The Usage and Security document also references the exception policy [353] giving department heads and unit IT personnel explicit direction as to where to learn about the rules for exceptions.

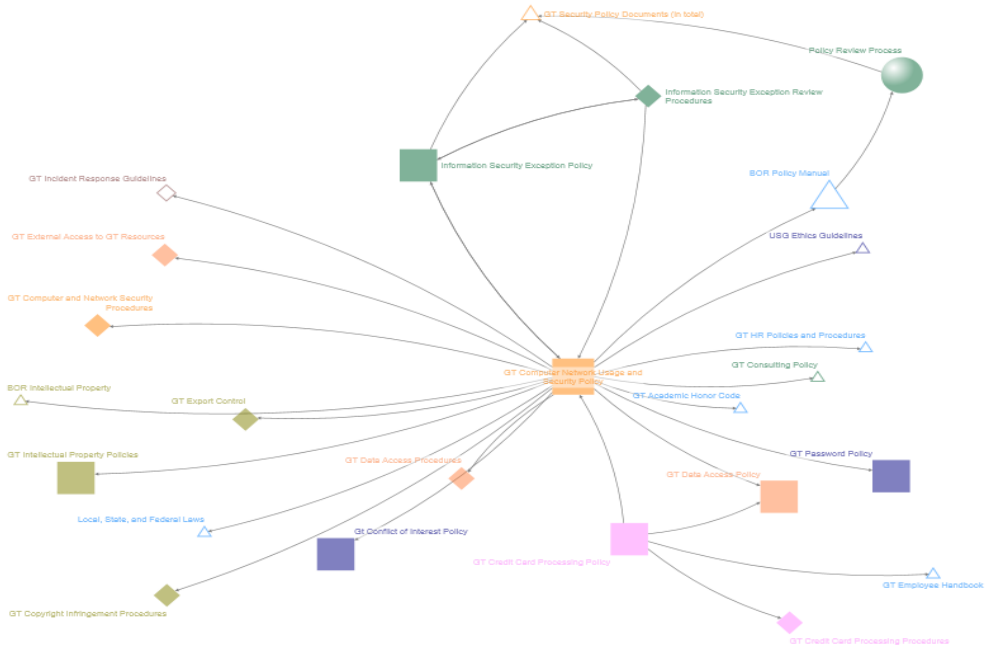

Figure 6-1 GT Policy Structure Graphic

Georgia Southern (GS) also presents a formal meta-policy in the document entitled IT Policy Development and Review Process [336]. However, the network structure displayed in the GS graph (Figure 6-2) shows a number of policy documents; Appropriate Use, Data Stewardship, Workstation procedures, and Copyright, attached to a small set of similar policies and procedures creating four “star” network configurations. There are no “horizontal” connections between the areas.

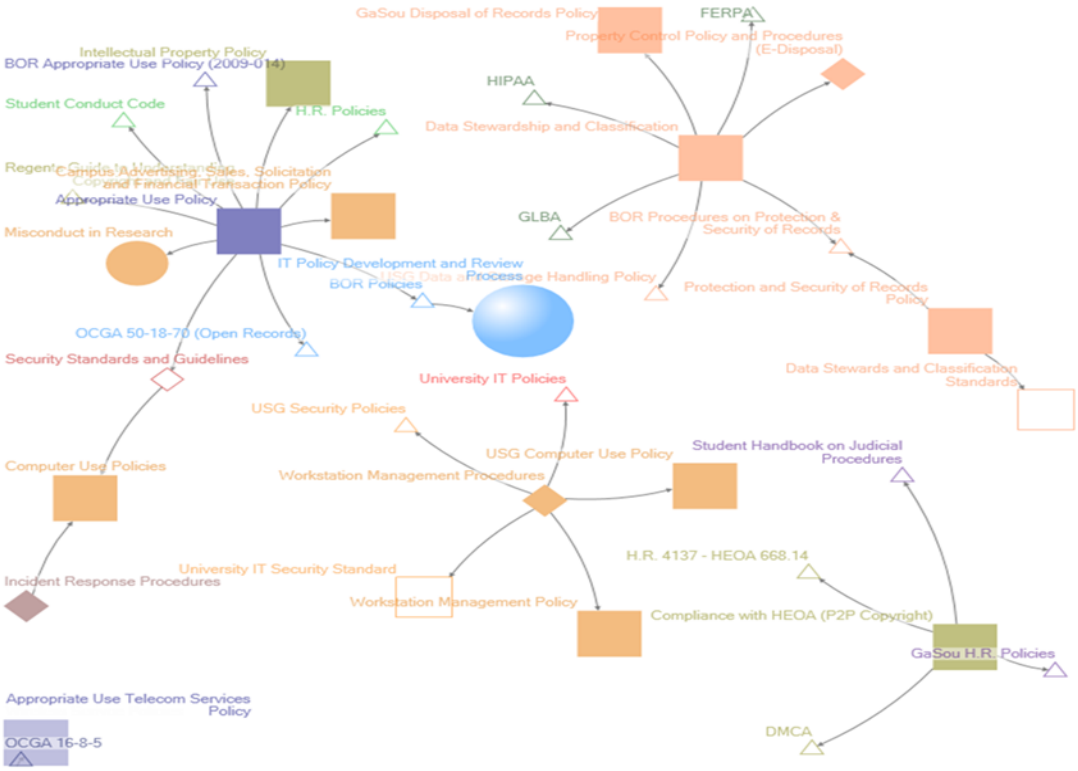

Figure 6-2 Georgia Southern Policy Structure Graphic

Similarly, the graph for UGA (Figure 6-3) shows areas of policy represented by an arrangement of procedures and ancillary documents referenced by a single policy document for each policy issue. In Chapter 5, I described the UGA strategy of referencing external policy requirements rather than integrating those requirements in a university-wide policy. Those references are identified by the triangles referenced by a UGA policy document. UGA has a single Acceptable Use policy that uses these references without providing procedures, guidelines, or other direction for campus employees and students. The UGA Password policy shows more components than any other area. The document was revised in 2011 and it is one of the newer policies

studied. The Secure UGA Plan [466], presented as a memorandum to UGA cabinet members, is a meta-policy, but one that has been abandoned.

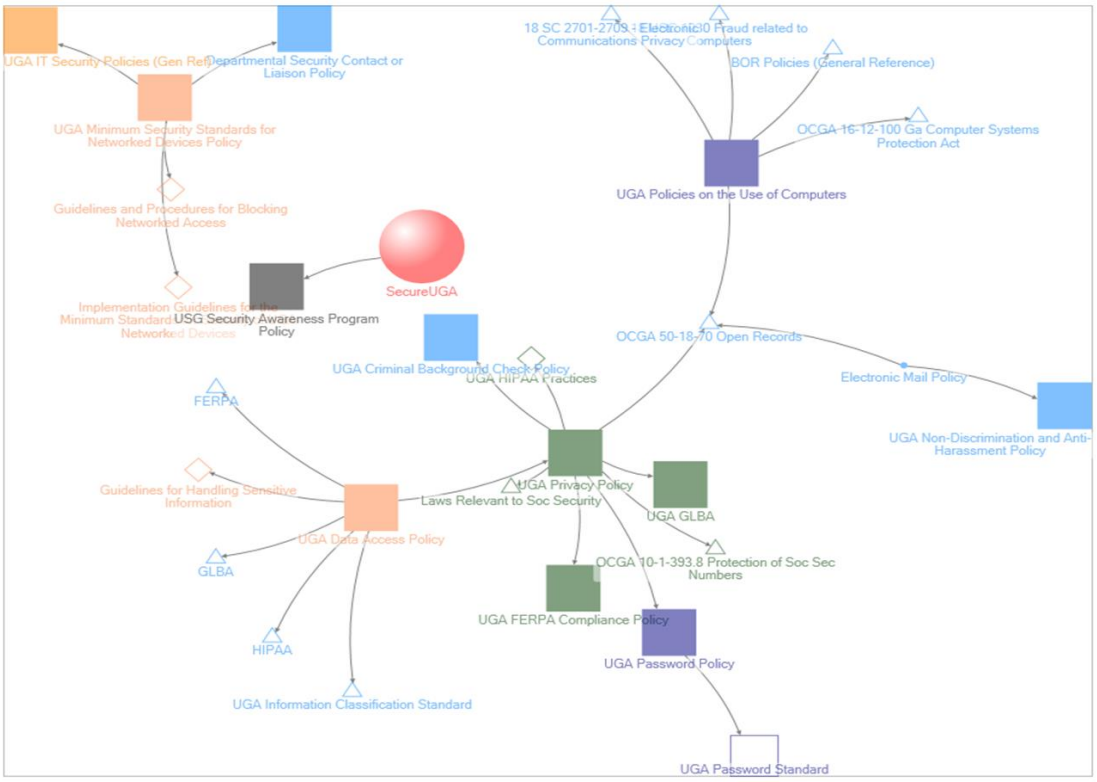

Figure 6-3 UGA Policy Structure Graphic

Finally, Georgia State (GSU) shows a strongly networked collection of documents (Figure 6-4). The central document, University Information Systems Use Policies [361], is a collection of policy issues referencing more specific policy documents that, in turn, reference procedures. A couple of horizontal connections are found between the Web Policy [374] and the Web Accessibility Policy [373]; and the Information Systems Ethics Policy [365] references the Information Security Management System policy (ISMS) [367]. The ISMS document reflects the processes defined by the ISO-27002 standards

for policy development that are employed by IT and two other departments of GSU. The document does not qualify as a meta-policy because the university did not adopt the policy for the entire organization.

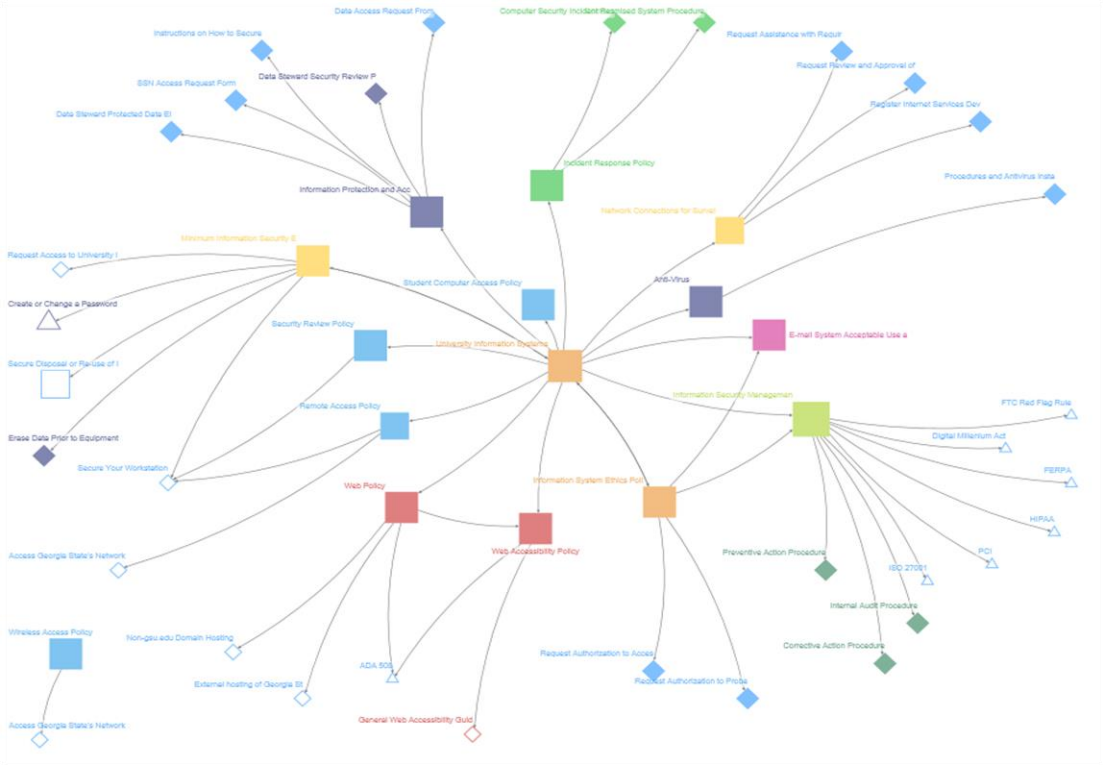

Figure 6-4 GSU Policy Structure Graphic

The literature suggests that a well-structured policy system would have each of the components represented. As the findings show, this is not the case. However, the components identified in the graphs are consistent with USG expectations, also described in Table 6-1. The USG does not mention a meta-policy, per se, nor does it describe procedures. However, the USG definition for standards combines the elements found in the literatures' definitions of standards and procedures. Each graph, especially

GT and GSU, present the components under the USG expectations. GT and GSU exhibit the strongest structuring using these components. UGA represents the weakest structuring.

The general document-level findings are not dissimilar from those discussed by Doherty (2009). The authors noted that universities tended to have an information security policy, accompanied by a number of related policies, and then also supplemented by a number of specific guidelines and/or practice-related documents" (Neil Francis Doherty, Anastasakis, and Fulford 2009, 453). The graphical analysis provides a succinct visualization of that finding.

Taking the analysis one step further, I examined the data in light of the criteria defining the network structure of the documents (Table 6-3). Georgia Tech's structure shows the strong influence of the meta-policy document and the discipline of creating university-wide policy versus the previous history of allowing colleges and departments to "opt out" of coverage as they saw fit. The case meets the minimum criteria of Formal structure. Given time, one can speculate that relative strength will improve.

An Ad Hoc structure is one that contains a general information security policy, accompanied by related policies. UGA's structure closely resembles this description. The meta-policy document for UGA, shown in the graph, is not in use. Georgia Southern has a stronger array of documents surrounding its Appropriate Use Policy, and it has an active, formal meta-policy. However, no horizontal linkages are found. This suggests a cluster network structure labeled as informal. However, the existence of a meta-policy suggests a stronger structure than most informal arrangements without such a policy.

Table 6-3 Policy Structure Criteria

Policy Structure	Description
None	Absence of general info sec policy, no links among policy documents
Ad Hoc (Loosely Coupled)	A general Information Security Policy, accompanied by a number of related policies and supplemented by specific guidelines and practice-related documents. Policy documents have little, if any, references to other existing policies
Informal (Cluster)	Policies and standards, supplemented by a number of related guidelines and procedures, with each guideline or procedure focused on one aspect of security mgt. The documents x-reference across types of security issues. . *A map of these policies demonstrates vertical links between policies, standards and procedures with few horizontal links connecting types of security issues. [emphasis mine].* A map of documents would present the horizontal links missing in the Ad Hoc structure.
Formal (Emergent)	A series of inter-related, cross-referenced policies (separate system, product, community, and corporate information security policies) –governed by a Meta Policy.

Georgia State (GSU) presents a central security policy document surrounded by a number of documents focused on particular policy issues which then reference standards and procedures. A couple of horizontal connections are evident between policies. The absence of a formal meta-policy places GSU has an in the informal category.

To summarize, using the above criteria, the findings suggest the following policy structures:

- GT – Formal
- GS – Informal (leaning toward formal)
- GSU – Informal
- UGA – Ad Hoc

The underlying claim to the research question is that the policy structure reflects the governance structure. So, an ad hoc policy structure is one that shows little coordination among policies focused on different cybersecurity areas of concern. A collection of policies that address acceptable use, password protection, data confidentiality, and others, will have little effect if those policies are not presented to

the staff and students in a well-structured awareness effort. Policies that do not take advantage of existing organizational procedures for implementation, monitoring, and enforcement are likely to be perceived as "not a priority" by individuals charged with operational decisions. If top management participation is not apparent, the perception that the policy is not among the organization's priorities is amplified. As structure improves, then some of these problems are mitigated. A formal policy structure suggests a documented approach to policy making that requires collaboration of all stakeholders, the education of individuals, and a concerted effort to fit cybersecurity policies within organizational goals, objectives and culture. The remaining hypotheses test these assumptions.

6.1.2 Measuring Structure –Categorizing Observations

Both measures, graphical and institutional, are crude measures of structure. Both indicate differences in structure among the cases. Units of observation are collected across several documents and across time for each case. The frequency analysis in Table 6-4 shows variation in the proportion of institutions observed within each Knapp process. Those proportions are a crude measure of structure by counting institutions. The Chi^2 statistic confirms that a relationship between institutional structure and organizational structure exists. In other words, it is unlikely that the proportion of observations that fall in to the Knapp processes are independent of the organizations that created them.

Table 6-4 Frequency Analysis - Observations within Knapp Processes

Action Situation	UGA	Ga Southern	GSU	GT	Row Total
Approval	19	3	19	9	50
	1.92	7.04	3.14	0.42	
	0.04	0.01	0.05	0.03	0.03
Awareness and Training	69	36	23	32	160
	13.76	0.29	7.63	0.38	
	0.16	0.09	0.06	0.09	0.10
Development	54	54	48	50	206
	0.16	0.21	0.35	0.36	
	0.12	0.14	0.12	0.14	0.13
Enforcement	39	44	19	5	107
	0.36	0.41	0.18	0.05	
	0.09	0.11	0.05	0.01	0.07
Implementation	215	221	237	197	870
	2.79	0.21	1.19	0.04	
	0.49	0.56	0.59	0.55	0.55
Monitoring	17	15	39	17	88
	2.23	2.05	12.44	0.35	
	0.04	0.04	0.10	0.05	0.06
Review	28	14	18	18	78
	1.90	1.41	0.16	0.02	
	0.06	0.04	0.04	0.05	0.05
Risk Assessment	1	4	2	28	35
	7.80	2.47	5.33	52.23	
	0.00	0.01	0.00	0.08	0.02
Retirement	0	2	0	0	2
	0.55	4.61	0.51	0.45	
	0.00	0.01	0.00	0.00	0.00
Column Total (N)	442	393	405	356	1596
N/Table Total	0.28	0.25	0.25	0.22	
Cell Contents **N** **Chi^2 Contribution** **N/Col Total**				Chi^2 = 166.5745 d.f. = 24 P = 2.59805e-23	

Table 6-5 Structure Determined by Presence of Knapp Processes

IAD Framework	Knapp Governance Model		Structure			Cases				
Level of Analysis	**Action Situation**	**Description**	**Ad Hoc**	**Informal Network**	**Formal Network**	**GS**	**GSU**	**GT**	**UGA**	**Avg**
Collective	Approval	Actions required to approve policy; to operationalize the policy	W	W	P	W 0.01	P 0.05	P 0.03	P 0.04	.03
Collective	Development	Activities include issue identification, definition of scope, research and analysis and stakeholder input	W	P	P	P 0.14	W 0.12	P 0.14	W 0.12	.13
Collective	Retirement	Removal of policy from active service	N	W	P	P 0.01	N 0.00	N 0.00	N 0.00	.00
Collective	Review	Management review of policy performance, alignment with business objectives, and effectiveness given other emerging technologies and security issues	N	W	P	W 0.04	W 0.04	P 0.05	P 0.06	.05
Collective	Risk Assessment	Identification of organizational values, policies that may be compromised if certain behaviors are allowed to occur	N	W	P	W 0.01	N 0 . 0 0	P 0.08	N 0.00	.02
Operational	Awareness and Training	Efforts to communicate to the campus community and to train them in the issues related to the policy in question	W	W	P	W 0.09	W 0.06	W 0.09	P 0.16	.10
Operational	Enforcement	Judgment of whether a violation of policy occurred; application of sanctions	N	W	P	P 0.11	W 0.05	W 0.01	P 0.09	.07
Operational	Implementation	Operational level application of the rules and norms contained within the policy document	W	P	P	P 0.56	P 0.59	P 0.55	W 0.49	.55
Operational	Monitoring	Observation of policy compliance, audits of systems, use of automated tools to scan for behaviors not allowed	N	W	P	W 0.04	P 0.10	W 0.05	W 0.04	.06
Legend: (P)resent; (W)eakly Present; (N)ot Present										

The analysis in Table 6-5 provides an opportunity to measure "relative strength" of processes. First, I classify a "Weak" structure one that has fewer statements in a process than the average of all cases. A "Present" structure has average or above statements. "N"o presence is coded when no statements are present for the process. Those values are then compared to expectations of structure presented in Table 6-5. Relatively speaking, Georgia Tech presents the strongest Knapp structure (4 Ps and 1 N), and Georgia Southern (GS) presents the second strongest. Georgia State and UGA present relatively weak Development processes. GSU also has a weak Review process, compared to UGA.

I measured the relative strength of policy structure by examining the results in Table 6-4 for deficient (missing or weak) Knapp processes. My measure is a simple count of Knapp processes for each case and whether the process strength maps to Formal, Informal, or Ad Hoc structure. I present two different counts in Table 6-6. The first count is of all Knapp Processes. The second count removes Retirement from the analysis. Retirement is absent from all cases, except for 2 observations found at Georgia Southern. Elimination of this one process adds some clarity to the structural differences.

Table 6-6 Knapp Process Tallies

Case	Formal	Informal	Ad Hoc
Georgia Tech (GT)	5 *5*	3 *4*	1 *0*
Georgia Southern (GS)	4 *3*	5 *5*	0 *0*
Georgia State (GSU)	3 *3*	2 *2*	4 *3*
University of Georgia (UGA)	3 *3*	2 *2*	4 *3*

The results are similar to the ones found when graphing the structure of documents. GT might be labelled a weak Formal, as the analysis by Knapp process adds some specificity not previously available. GS is a strong Informal. GSU and UGA are similar – which would demote GSU to Ad Hoc status.

My first hypothesis expected Policy structure to be a reflection of Governance structure. The previous section examined the measurement of policy structure using document and statement analysis. My second hypothesis expects a correlation between governance structure and the presence of formal meta-policy:

> **H2**: If an organization possesses a meta-policy then the likelihood that that organization observes most if not all of the processes identified in the Knapp model is greater than an organization without a meta-policy.

I examine a correlation between the Knapp structure of governance and whether that organization possesses a formal meta-policy document. Table 6-6 summarizes the Knapp collective level processes observed for each case.

Table 6-7 Observed Knapp Processes - Relative Strengths

	UGA	**GS**	**GSU**	**GT**
Approval	P	W	P	P
Development	W	P	W	P
Retirement	N	P	N	N
Review	P	W	W	P
Risk Assessment	N	W	N	P
Legend: “N”o process, “W”eak process, “P”rocess Present				

The two cases with a meta-policy document, GT and GS, demonstrate an observance of most Knapp processes. I compare the expected strength of processes found in Table 6-5 for collective level (governance) processes. GT is deficient in the

Retirement process, but codes as a Formal structure in all other processes. The relative strength of GS processes map closely to Informal, although its Retirement process is stronger than necessary. UGA and GSU have no statements observed that code for Risk Assessment and Retirement. And, they are both relatively weak in Development. Neither UGA nor GSU have a formal meta-policy for information security in use. The relative strength of GT compare to GS, UGA, and GSU suggests there is merit to the premise of Hypothesis 2.

6.1.3 Differences in Components

The precision of analysis may improve as we move from documents to statements and identify these components. The grammatical analysis of statements found in policy documents provide data to align those statements with the types of policy components identified by multiple researchers. As the governance structure becomes more formal, I expect the structure of policy will present a more complete set of policy components necessary for effective security.

> **H3:** An effective formal governance structure presents a full complement of components and Knapp processes to be effective.

A frequency analysis of policy components (Table 6-8) tests this hypothesis. Georgia State (GSU) has the largest proportion (29%) of policy statements coded as metapolicy statements. UGA and GSU have similar proportions (17%) while GT metapolicy statements occupy 22% of the total statements identified (Table 6-7). Analysis shows that 24% of GSU governing statements are identified with Approval, by far the largest proportion of any case. GSU also demonstrates the smallest proportion

of statements in the Development action situation with 43% of statements regulating activities to develop policy. The other three cases show roughly similar proportions ranging from 55% (GT) to 64% (UGA).

Table 6-8 Distribution of Observations as Components

Policy Type	UGA	Ga Southern	GSU	GT	Row Total	Cell Contents
Ancillary	6	3	1	2	12	**N**
	1.55	0.01	0.70	0.28		**Chi Square Contribution**
	0.50	0.25	0.08	0.17	0.01	**N/Row Total**
	0.01	0.01	0.00	0.01		**N/Col Total**
Guideline	42	10	9	19	80	
	13.09	6.08	2.44	0.01		Chi^2 = 81.24561
	0.52	0.12	0.11	0.24	0.05	
	0.10	0.03	0.03	0.05		d.f. = 15
Procedure	78	135	49	93	355	
	8.05	16.84	4.75	0.61		p = 4.131141e-11
	0.22	0.38	0.14	0.26	0.24	
	0.18	0.35	0.18	0.26		
Standard	132	100	74	70	376	
	2.93	0.00	0.15	4.78		
	0.35	0.27	0.20	0.19	0.26	
	0.30	0.26	0.27	0.20		
Policy	110	75	63	93	341	
	0.45	2.90	0.02	1.37		
	0.32	0.22	0.18	0.27	0.23	
	0.25	0.19	0.23	0.26		
Metapolicy	74	68	79	76	297	
	2.80	1.66	9.54	0.25		
	0.25	0.23	0.27	0.26	0.20	
	0.17	0.17	0.29	0.22		
Column Total	442	391	275	353	1461	
	0.30	0.27	0.19	0.24		

Graphing the distribution of components as a percentage of the total statements observed (Figure6-6) shows that the two cases with formal meta-policy documents, GT and GS, share similar distributions of statements across the components from meta-policy through procedure. The variance in proportions, and the direction of that variance are similar for GT and GS. UGA and GSU, the two cases that do not have formal

meta-policies in use, show similar behaviors both in quantity and direction of change in proportions as well.

UGA and GSU are similar in the representation of components with the exception of use of guidelines, where UGA is superior to GSU. UGA and GSU seem to be biased to expressing policy in terms of statements that define specific requirements that must be met by all individuals. GT and GS show a balance between outlining organizational and management responsibilities (meta-policies and policies) and those specific requirements found in standards and guidelines. Such a distribution is consistent with the relative strengths of Knapp processes measured above.

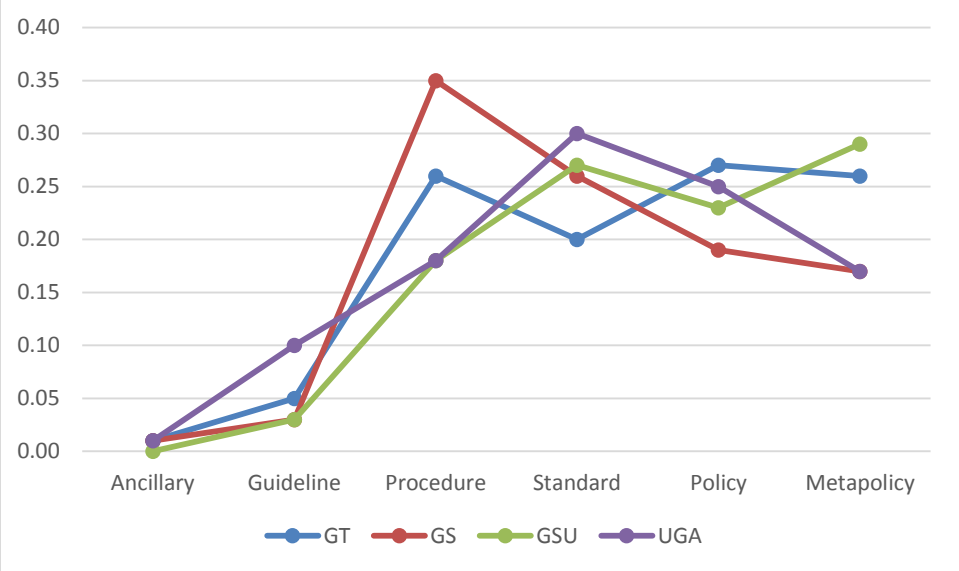

Figure 6-5 Distribution of Components

The third hypothesis is not supported in this analysis. Most of the data points are within 1 standard deviation of the mean for each component. GSU and UGA tend to track closely together in the proportion of statements identified in each component.

Outside of that pattern, you cannot attribute the presence of policy components to formality of structure.

6.1.4 Dialing in Precision

The next set of hypotheses test variations in structure by examining meta-policy statements within the distinct tasks that the ACUPA model proposes (Table 6-9). I identified the ACUPA step for each statement by aligning the aIm with the task description for each step. Each statement was also coded for rule type using the criteria discussed in chapter 4. The statements grouped by the appropriate ACUPA steps are shown in tables identified by case in the appendix[41]. The total number of metapolicy statements for each case is similar, the graph (Figure 6-6) showing the proportion of observations within each ACUPA Action Situation shows the different emphasis on specific governance tasks for each case.

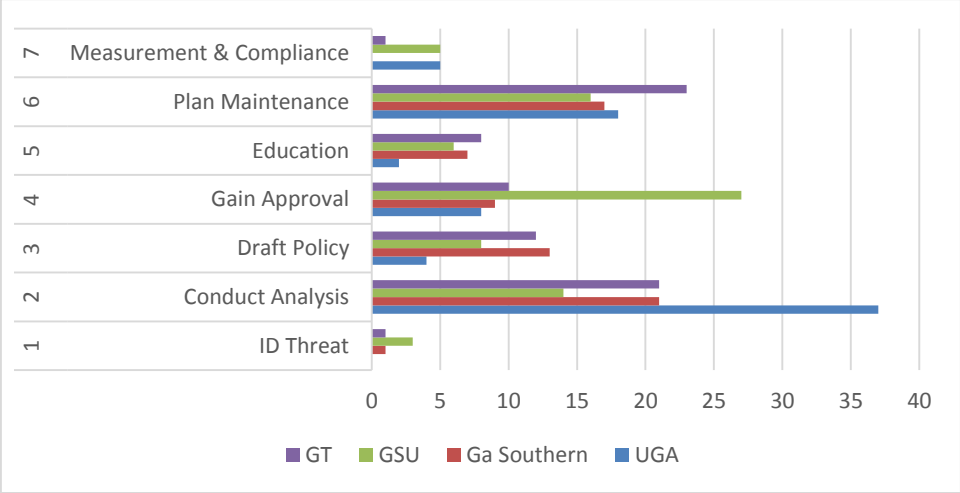

Figure 6-6 Distribution of Statements by Case (N=297)

[41] Georgia State (GS) – Appendix J; Georgia Southern (GSU) – Appendix K; Georgia Tech (GT) – Appendix L; UGA (UGA) – Appendix M

Table 6-9 Rules Configurations per ACUPA Step

ACUPA	Description	Ga Southern							GS Tot	GSU							GSU Total	GT							GT Total	UGA							UGA Total	Grand Total
		Aggregation	Boundary	Choice	Information	Payoff	Position	Scope		Aggregation	Boundary	Choice	Information	Payoff	Position	Scope		Aggregation	Boundary	Choice	Information	Payoff	Position	Scope		Aggregation	Boundary	Choice	Information	Payoff	Position	Scope		
1.01	Scans for changes in law, threat, best practices, etc.	0	0	0	0	0	0	0	0	0	0	2	0	0	0	0	2	0	0	0	1	0	0	0	1	0	0	0	0	0	0	0	0	3
1.02	may identify need/issue	0	1	0	0	0	0	0	1	0	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2
2	Miscellaneous	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	0	0	0	0	0	0	0	0	1
2.01	Identify Owners	0	2	0	0	0	2	0	4	0	0	0	0	0	2	0	2	1	0	1	1	0	0	0	3	0	2	3	0	0	1	0	6	15
2.02	Determine Path (Policy Plan – Scope Definition)	0	0	2	0	1	0	0	3	0	0	1	0	0	0	0	1	0	0	1	0	0	0	0	1	2	0	1	0	0	0	1	4	9
2.03	Assemble Team	0	3	0	0	0	0	0	3	0	1	2	0	0	0	0	3	0	8	0	0	0	0	0	8	0	3	1	0	0	11	0	15	29
2.04	Gather Data	0	0	1	0	0	0	0	1	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	2	0	0	0	0	2	4
2.06	Determine Risks	0	0	1	0	0	0	0	1	0	0	2	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1	4
2.07	Determine Stakeholders	0	2	0	0	0	1	0	3	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	0	1	0	0	0	2	0	3	7
2.08	Determine solutions	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1	0	0	2	0	0	0	0	2	0	0	2	0	0	0	0	2	5
2.09	Can present policy be revised?	0	0	3	0	0	0	0	3	0	0	2	0	0	0	0	2	0	0	0	1	0	0	0	1	0	0	1	0	0	0	0	1	7
2.10	Determine need for new policy	0	0	1	1	0	0	1	3	1	0	1	0	0	0	0	2	0	0	0	0	0	0	4	4	1	0	2	0	0	0	0	3	12
3.01	Agree on Definitions	1	0	1	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	3
3.02	Drafts Policy -Use Common Format	1	1	2	0	0	0	0	4	0	0	4	0	0	0	0	4	0	0	1	1	0	0	0	2	0	0	0	0	0	0	0	0	10
3.03	presents drafts to stakeholders	0	0	0	5	0	0	0	5	0	0	1	2	0	0	0	3	0	0	0	2	0	0	0	2	0	0	0	1	0	0	0	1	11
3.04	review and vet proposals	0	0	1	0	0	0	0	1	0	0	1	0	0	0	0	1	0	0	0	5	0	0	0	5	0	0	2	0	0	0	0	2	9
3.05	presents to policy advisory Committee	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	1	2	0	0	0	3	0	0	0	0	0	0	0	0	4
4.01	Presents policies for approval to advisory committee	0	0	0	2	0	0	0	2	0	1	3	2	0	0	0	6	0	0	0	1	0	0	0	1	0	0	0	0	0	0	0	0	9
4.02	Considers/approves/modifies proposals	0	0	0	0	0	0	0	0	1	0	8	0	0	4	0	13	0	0	2	0	0	0	1	3	1	0	0	0	0	0	0	1	17
4.03	collects comments/revises as needed	0	0	2	3	0	0	1	6	0	0	3	1	0	0	0	4	0	0	0	5	0	0	0	5	0	0	0	0	0	0	0	0	15
4.04	Obtain Approvals	0	0	0	1	0	0	0	1	4	0	0	0	0	0	0	4	1	0	0	0	0	0	0	1	5	0	2	0	0	0	0	7	13
5.01	Plan Communications	0	0	2	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	0	0	1	0	0	0	0	1	4
5.02	Put online	0	0	0	1	0	0	0	1	0	0	1	2	0	0	0	3	0	0	0	4	0	0	0	4	0	0	0	0	0	0	0	0	8
5.03	Provide searches	0	0	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
5.04	Communicates policy to audiences	0	0	0	3	0	0	0	3	0	0	0	3	0	0	0	3	0	0	0	3	0	0	0	3	0	0	1	0	0	0	0	1	10
6.01	Versions new policy	0	0	1	0	0	0	0	1	0	0	0	4	0	0	0	4	0	0	2	0	0	0	0	2	0	0	0	0	0	0	0	0	7
6.02	Archives old policy	0	0	2	1	0	0	0	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3
6.03	Establishes schedule for review	0	0	1	0	0	0	0	1	0	0	0	1	0	0	0	1	0	0	2	0	0	0	0	2	0	0	7	0	0	0	0	7	11
6.04	Determines review procedures	0	0	4	0	0	0	0	4	0	0	2	7	0	0	0	9	2	0	1	1	0	0	0	4	2	2	4	0	0	0	0	8	25
6.05	solicits feedback	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	2	2	0	0	0	5	0	0	3	0	0	0	0	3	8
6.06	Reviews risk and Cost	0	0	4	0	0	0	0	4	0	0	0	0	0	0	0	0	0	0	8	0	0	0	0	8	0	0	0	0	0	0	0	0	12
6.07	Recommends whether policy still needed	2	0	2	0	0	0	0	4	1	0	1	0	0	0	0	2	1	0	1	0	0	0	0	2	0	0	0	0	0	0	0	0	8
7	Miscellaneous	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	1
7.01	Measures/monitors outcomes	0	0	0	0	0	0	0	0	1	1	3	0	0	0	0	5	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1	6
7.02	Enforcement	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3	0	1	0	0	0	0	4	4
(blank)																																		
Grand Total		**4**	**9**	**30**	**18**	**2**	**3**	**2**	**68**	**9**	**3**	**39**	**22**	**0**	**6**	**0**	**79**	**5**	**9**	**24**	**32**	**0**	**0**	**6**	**76**	**15**	**8**	**35**	**1**	**0**	**14**	**1**	**74**	**297**

The relevance of Table 6-9 is how it summarizes the differences in structure among the cases for each ACUPA step. The table succinctly presents the types of rules that each case employs to accomplish the objective of that step. The configuration of rule types (i.e. number of Choice, Information, Scope rules) defines the context within which actors make the decisions that are linked together as the tasks are completed to create policy decisions. In the next section, I highlight the role that the grammatical components play in determining and identifying the signature features of governance structure for each case. The "actor" for each step is included to complete the set of data required to understand the structure of each task.

6.2 Organizational Conditions – Differences Compared

Organizational conditions are described in the development of the research framework (Ch. 2) and the discussion of hypotheses (Ch. 3). Two of the most influential conditions, Top Management Support and Collaboration, are analyzed as they are the most likely to affect the structure of governance and policy for the cases.

6.2.1 TMS

Top Management Support (TMS) is a criteria for success that is prevalent in the literature and in the security standards (PCI, ACUPA, ISO) described in chapter 5. Institutions are employed to select agents acting on behalf of an organization in different decision contexts (McGinnis 2011b, 54). The influence of top management support is reflected in the institutions that govern behavior (Purvis, Sambamurthy, and Zmud 2001). The absence of visible top management support is linked to ineffective

policy and ineffective or weak cybersecurity (Chan, Woon, and Kankanhalli 2005; Goo, Yim, and Kim 2013; Thong, Yap, and Raman 1996; Kankanhalli et al. 2003b; Hu et al. 2012).

I suggested in chapter three that the number of principals of the organization within the governance structure is a proxy for Top Management Support (TMS). If all of the vice presidents of a college are engaged in the policy making decisions, then it is reasonable to expect that the structure of cyber security governance will approach the emergence level (i.e. tailored to the organization, able to respond easily to changing external and organizational conditions). The review of standards (PCI, ISO, AGILE) support this proposition. Requiring actors to participate may be seen as action on the part of top management to make security a priority of the organization.

6.2.1.1 TMS Findings

I created a categorical variable to assign the Attribute of each institutional statement into categories of: Individual, Top Management, Organization, and Vendor[42]. The distribution of Attributes within metapolicy statements for each organization is shown in Table 6-10. Georgia Southern shows an overwhelming percentage of Attributes coded as Top Management (85%). Almost 3 of every 5 UGA metapolicy statements identify a member of Top Management as Attribute, while 34 percent of GT statements and 29 percent of GSU statements identify as TMS.

UGA and Georgia Southern are more likely to assign responsibility for policymaking to top management positions while Georgia Tech and Georgia State are

[42] The criteria for variable assignment for Attribute Category is found in Appendix H., Table 1

more likely to assign the responsibility to an organizational entity (e.g. department, division, or the university. The president of every campus is bound to participate with the position of final approver (as the USG rule holds the president responsible for policy compliance).

Table 6-10 Attribute Category by Case

Category	UGA	Ga Southern	GSU	GT	Row Total
Individual	1	2	3	0	6
	0.16	0.29	1.24	1.54	
	0.17	0.33	0.50	0.00	0.02
	0.01	0.03	0.04	0.00	
	0.00	0.01	0.01	0.00	
Organization	29	8	53	50	140
	0.99	18.05	6.67	5.61	
	0.21	0.06	0.38	0.36	0.47
	0.39	0.12	0.67	0.66	
	0.10	0.03	0.18	0.17	
Top Mgt	44	58	23	26	151
	1.08	15.88	7.34	4.13	
	0.29	0.38	0.15	0.17	0.51
	0.59	0.85	0.29	0.34	
	0.15	0.20	0.08	0.09	
Column Total	74	68	79	76	297
	0.25	0.23	0.27	0.26	

Pearson's Chi-squared test

Chi^2 = 62.96843 d.f. = 6 p = 1.120226e-11

Cell Contents

N
Chi-square contribution
N / Row Total
N / Col Total
N / Table Total

An analysis of the cases revealed that all boundary rules were compulsory but for those that left it up to an actor to invite actors to participate (Table 6-11).

Table 6-11 Boundary Rules establishing teams

Actor	Georgia Southern	Georgia State	Georgia Tech	UGA
President	1st Order (USG)	1st Order – USG	1st Order – USG	1st Order – USG
CIO	1st Order	1st Order	1st Order	1st Order
CISO	Invite CIO	*1st Order*	1st Order	1st Order
Legal Affairs	Invite CIO	1st Order	1st Order	1st Order
Internal Audit	Invite CIO	*1st Order*	1st Order	1st Order
Faculty and Research			Invite CIO	1st Order
Bursar			Invite CIO	1st Order
Extended Campuses			Invite CIO	1st Order
Finance	Invite CIO	*Invite*	1st Order	1st Order
Human Resources	Invite CIO	*Invite*	1st Order	1st Order
Public Affairs	Invite CIO			1st Order
IT – Policy Compliance	NA	NA	1st Order	NA
Registrar	Invite CIO	Invite	1st Order	1st Order - PCI
IT – Enterprise	Invite CIO	Invite	1st Order	*Invite CISO*
Subject Matter Experts	Invite	Invite	1st Order	Invite - CISO
Policy (Process) Owners	Invite CIO	*Invite CISO/CIO*	*Invite CISO/CIO*	Invite - CISO
Stakeholders	Invite CIO	*Invite CISO/CIO*	Invite CISO	Invite CISO
Others	Invite CIO	*Invite CISO/CIO*	Invite CISO	Invite -CISO

UGA has significant and compulsory participation of TMS per the formal rules. However, interview data acknowledges that model is not the routine. The rules-in-use at UGA keep the top management informed, but avoid the formality of policy development by electing to reference externally mandated requirements. Georgia State formally engages top management once policy is proposed through the University-wide Policy process. The Information Security Management System, the metapolicy document based on the ISO 27002 standards, is employed by only 3 departments at

GSU, two of those are IT departments. Engagement of TMS in the identification of issues and in the analysis is minimal. Georgia Southern and Georgia Tech are found to have rigorous TMS within their respective systems. Georgia Southern employs a mostly informal metapolicy based upon the AGILE philosophy with some formal rules found in the IT Policy and Development Review Process document [336]. Georgia Tech has a formal metapolicy which is found to be used consistently.

6.2.1.2 Assessment of TMS Effects

I explored three hypotheses that suggest a simple relationship between the formality of policy structure, how many Knapp processes are present, and the numbers of top management officials that participate in the policy process.

> **H4a**: Governance structure will resemble the ideal Knapp model as the number of principals identified in 1st order boundary rules increase.
>
> **H4b**: High TMS is likely accompanied by compulsory Boundary rules requiring the participation of a number of principals of the organization.
>
> **H4c**: If there are no compulsory boundary rules, then the likelihood that a techno-centric governance process increases. TMS will be "lower" than in organizations with compulsory boundary rules.

A review of the counts of statements observed within Knapp Action situation (Table 6-4) and the TMS actors identified (Table 6-10) does not lead to a clear conclusion concerning the first hypothesis. The basic premise suggests that an effective governance structure is more likely to be present when TMS support is high because the managers will not waste time and resources on ineffective procedures.

Simple counts don't provide enough information to draw conclusions. The distribution of observations do vary by case, but there is not enough data based on

counts alone to draw conclusions. Each case has Knapp situations with very few statements, and the Development situation is generally robust.

However, adding context and identification of key features suggests some conclusion may be drawn on the relationship of TMS and Knapp structure. GSU invests 24% of observed metapolicy statements into the process of policy approval. All but one of those approval observations (see Appendix P) occur only if a policy reaches the Policy Advisory Group formed on behalf of the faculty senate under the University Wide Policy on Policies [475]. The interview with the GSU CISO indicated that the CIO would present a draft policy [470:12] only after the Office of Legal Affairs deemed the policy change as necessary [470:7] (see Appendix M). And, until that approval is gained, the process for developing security policy at GSU rests with the efforts of the CISO. There is no formal process to bring actors together to initiate a policy review until the CISO gets the Office of Legal Affairs to agree that a new policy or policy revision is necessary. This finding suggests that TMS support is weak in the GSU structure and that the policy process, as it is, is IT centric. The finding also fits the ideal of a "feature" which sets one map of institutions apart from another (Aligica 2006).

UGA presents strong, compulsory rules developed at the behest of the auditors from the Payment Card Industry (see documents 466 – SecureGA Plan and 472 – UGA Security Committee Charter). The first-order compulsory rules identifying TMS actors to participate are set by those documents. However, the interview [471] with the UGA CISO indicated the team of top management is not active. Review of the statements grammatical components in Appendix M – "Conduct Analysis" shows that CIO and CISO

as the most active actors and the actors responsible for inviting other team members to participate.

The norm for complying with external mandates for policy change is to reference those mandates within the UGA policies [471:16]. In fact, the statement noted that policy restating external requirements was forbidden. Simply referencing the external document in user agreements helped the organization avoid the time and resource consuming processes necessary to gain consensus to adopt a revised policy tailored to the UGA organizational conditions[43]. As is the GSU case, the actors are from the IT domain and TMS support is not required for the references to be made in lieu of a formal policy process.

Georgia Tech and Georgia Southern demonstrate strong engagement of TMS. Georgia Southern relies mostly upon the norms found within the AGILE philosophy (described in Chapter 5). Georgia Tech formally requires participation of upper management on the committee that decides whether the policy process is initiative, and if so, decides when the policy process has produced an outcome to be forwarded to the cabinet and President for final approval. The GT process also sets expectations that the Compliance Manager, in concert with the CISO and CIO, work to keep all appropriate sub-divisions of the university engaged in the drafting, revision, approval, and awareness processes. Notably, both organizations reported that the time required to

[43] Of course, this rule also raises the prospect that autonomy is a strong organizational condition to be managed in the process.

produce a policy was reduced to a period of 4 to 6 months. A contrast to the timetable of 18-24 months noted by the CISOs at UGA and GSU.

An examination of the institutions governing actors, top management, and collaboration adds information to the determination of the influence of TMS in these cases. Criteria examining how actors defined in TMS are engaged is presented in Table 6-12. Based on these criteria, the structure is determined to be Formal, perhaps leaning towards informal.

Table 6-12 Collective Level Structure Assessment

CRITERIA	ASSESSMENT	GT	GS	GSU	UGA
ACTORS REPRESENT THE SUB-UNITS AND INDIVIDIUALS WITHIN THE ORGANIZATION	Rules-in-use require engagement of entire organizational structure, diverse actors	Yes	Yes	No	No
TOP MANAGEMENT SIGNIFICANTLY ENGAGED (BY NUMBER OF ACTIONS AS ATTRIBUTE, IDENTIFIED IN COMPULSORY BOUNDARY RULES	Formally identified as Attribute responsible for actions; boundary rules are mostly compulsory	Yes	No Via Invitation	No	No
FINAL ASSESSMENT		Strong TMS	TMS	Weak TMS	Weak TMS

This evaluative criteria connects the observations of institutions with actors. The data from GT supports all three hypotheses. The policy process [360] provides strong formal relationships between TMS actors and the process, defining areas of engagement, and ties to outcomes. The process document describes the steps acknowledged by the Knapp model to be necessary for effective policy governance, with the exception of a formal retirement policy. Georgia Southern provides evidence that a norm-driven philosophy can be as successful as the formal structure provided at GT. While the actors of sub-units are not required by rule, the process does include these

stakeholders and TMS as well. The rules-in-use, as Ostrom and others have noted, are the observations which matter. At GT the rules-in-form are, largely, the rules-in-use.

GSU and UGA indicate that rules-in-use are not necessarily the same as rules-in-form. As the criteria suggest, TMS in both cases is relatively weaker than TMS found at GT and GS. GSU demonstrated in the three sub-divisions that adopted the formal ISO-27002 standards how effective policy can be in regulating behavior. However, in the other areas of GSU that reside under the "umbrella policy" philosophy of the Office of Legal Affairs, alignment of organizational policy with external mandates has not occurred. The removal of the observations from the Information Security Management System document [367], developed for the ISO 27002 implementation, and the University-Wide Policy on Policies [475], eliminates 70% of the formal metapolicy observations as well as almost all the TMS actors found in those attributes. The governance structure is largely ad hoc, supporting the premise of all three hypotheses.

UGA also provides evidence that the active engagement of TMS makes a difference in the governance structure. TMS support is formally required in the two documents created as an outcome of collaborating with the Payment Card Industry. But, outside of the security policies directed at credit card information, the TMS levels drop back to an IT centric model of policy governance. The quick answer to new policy mandates is to place a reference in existing policy. The lack of TMS is observed in this Choice rule directing that no tailoring, no formatting, no scoping be applied to align the external policy to UGA conditions. Governance structure is not as strongly aligned with

the Knapp model as the GT and GS structures are. Without strong TMS, the first three hypotheses are supported.

Clearly, the presence of first order rules-in-form does not guarantee strong TMS influence within an organization. It is apparent that "Rules-in-use" may construct an entirely different set of actors than those found in the written documents. Therefore, Hypothesis 4a is not clearly supported. When I focused on rules-in-use, then the number of compulsory boundary rules requiring diverse yet influential participation of Top Management aligned with the data on formality of structure. Georgia Tech shows the strongest TMS influence. Georgia Southern shows weak formal TMS influence, yet the practice, as guided by AGILE, provides a relatively stronger influence of TMS than GSU or UGA. Hypothesis 4b is supported. The interview data of the latter two cases confirmed a largely techno centric approach to policy making. Both UGA and GSU present the weakest governance structures. Hypothesis 4c is supported by this evidence.

6.2.2 Collaboration and Autonomy

Theory suggests that in addition to TMS, collaboration among the stakeholders is an important criteria for development of effective policy. However, autonomy of departments and divisions may defeat the positive effects of collaboration and frustrate policy effectiveness. Tailoring the content of policy to align with organizational objectives, culture, and other conditions improves effectiveness. Tailoring occurs when stakeholders are able to submit modifications that are adapted via a feedback mechanism that includes comment collection, re-drafting, and a review

by those same stakeholders to inspect whether the modifications were accepted. The form of policy content is also more likely to align with the needs of stakeholders if those same stakeholders review the content prior to publication. So, tailoring depends upon strong collaboration between top management, security managers, and stakeholders.

6.2.2.1 Open Boundary Rules

"Open" boundary rules allow individuals flexibility to enter and leave action situations based on their desire to participate. The invitation boundary rules are the type of "open" boundary rules thought to encourage collaboration. Hypothesis 5a examines the relationship between rules that set criteria to guarantee participation of individuals affected by a potential rule to participate.

> **H5a**: The presence of Open Boundary Rules setting the criteria for participation in making security policy reflects an organizational condition that values collaboration. An Ad Hoc structure will be the least likely to present Open Boundary rules. A Formal structure is likely to present Open Boundary Rules.

The findings suggest that "openness" varies by case. The rules that set the criteria for participation are found in Appendix N – "Conduct Analysis" and Appendix O – "Draft Policy". At UGA, the CISO and CIO set the agenda and scope of policy development in "consultation with stakeholders" [471:14]. Those stakeholders are identified and invited on an ad hoc basis [471:7]. And, the CISO refines the strategy for developing policy in consultation with team members [471:3].

A similar criteria is employed at GSU to select individuals to participate in the "early" analysis prior to the critical decision by the Office of Legal Affairs as to whether new policy is need (and thus invoking the wider "University Policy on University-Wide

Policies"). The CISO indicated that the Office of Legal Affairs preferred the Network Standards Policy [368], adopted in January of 2004, in lieu of new policy, if it all possible. Per this "umbrella policy", the CISO is the individual responsible for working with Information resource owners, data administrators, and "functional" users to develop policy [368:3]. "Functional" users is a vague term that refers to those using an application in the course of the business day. Observation 361:20 provides that the Information Technology Senate Sub-committee has responsibility to decide upon changes to policies. However, the CISO stated that committee had not met in many years after the departure of its last chair. Opportunities for other stakeholders to participate are not defined under these procedures.

The rules-in-use at Georgia Southern are driven by AGILE design principles to take input, turn around modified policies, and achieve approvals across these groups in a network of activity versus pushing drafts of policy through a top-down structure of communication. The AGILE design approach focuses on consensus rather than authority. While the formal rules for policy development are non-symmetric (i.e. top-down management decisions), the informal rules are symmetric, allowing the actors to work towards consensus using flows of information to inform group decision-making. The feedback encouraged by AGILE reflects the Circular processes in the Knapp model which both practice and theory acknowledge as necessary for effective policy.

Collaboration by the many stakeholders in the GT policy process is encouraged both formally and informally. A number of observations implicitly define who may enter the action situation as stakeholders (ACUPA 2.07 [360:27]), to advise on drafts

(ACUPA 3.03, [360:30]), to vet proposals (ACUPA 3.04, [476:4]) and to approve (e.g. ACUPA 4.03, [476:8])[44]. There are also actors that participate in the policy process due to their position in adjacent action situations (budgeting, institutional research boards, etc.).

Information rules requiring the distribution of policy drafts and evidence supporting the policy drafts indirectly create opportunities for participation[45]. The Policy Review Policy [360] requires the Policy Compliance Manager (PCM) to communicate all prospective changes to the community representatives, and to seek input from the same. The CIO is required to discuss policy proposals with the executive leadership team [476:1]. Drafts of the proposals must be discussed among members of the Policy Review Committee [360:37], meet with data stewards and policy owners [476:3], Human Resources and Legal Affairs [476:11], deans and unit IT directors [476:6], the faculty senate committee [476:7], the faculty executive board [476:7], and seek input from a variety of technical communities on campus [360:27]. The PCM must socialize draft policies with the student government, faculty members, and the PRC and solicit feedback from those groups [360:28-30]. The Policy Review Committee has to provide "feedback and constructive criticism" within the context of their individual

[44] In the final chapter, I discuss a proposed methodology change to allow assigning of multiple rule types, action situations, and policy areas to a unit of observation and how that may increase the descriptive power of this approach.

[45] This is an example of observations that are directly coded as one rule type (information) that by inference create another rule type (boundary). In this case the OBJECTs of the rule (sharing and feedback of information) are the stakeholders from whom the Attributes are expected to receive information and support. Clearly, informal rules exist to "open" the participation to many who care, and others, who by title, have responsibility for areas affected by the proposed draft. I will discuss this item further in proposed future research regarding the methodology.

functional responsibilities [360:13-14]. Finally, the policy must be published in a manner that facilitates access by the entire campus [344:71, 353:26,353:29,360:38-39].

As the sequence of findings ranging from UGA to GT suggest, as the participation in the process becomes more open, the Knapp processes become more explicit in the depth of the activities for development, risk assessment, and review of policies. The GS and GT actions found in Appendices M and N display a more diverse configuration of Choice, Information, and Scope rules than UGA or GSU. The opportunities recognized to include stakeholders in the observations for UGA and GSU decrease significantly when the observations are limited to "rules-in-use". At the same time, the relative strength of GT and GS rules-in-use for open participation remain strong. The evidence supports Hypothesis 5a.

6.2.2.2 Absence of Invitation Rule – indicates ad hoc structure

> **H5b**: The absence of an invitation boundary rule specifying participation of university leadership will increase the likelihood of a governance structure that is largely ad hoc in nature.

The hypothesis expects that unless an invitation boundary rule specifies university leadership then you are more likely to find an ad hoc policy governance structure. The findings for Hypothesis 5b, based on observed data (Table 6-11) alone suggest that GS and GSU are more likely to have Knapp deficient structures while GT and UGA will have more complete governance structures. A comparison of Georgia Southern and UGA institutions (Appendix M) suggests the relationship between the participation of leadership specified by boundary rules and structure is not this simple.

There are three tasks identified in the ACUPA model (Table 6-4) that specifically identify policy owners (2.01), policy team (2.03), and policy stakeholders (2.07). Both GS and UGA have similar counts of Boundary rules. However, UGA has far more observations (24) in these three areas than GS (10). A significant number of observations are coded as Position rules for Step 2.03 "Assemble Team".

Coding rule types is done based on the verb form of the aIm component of the observation. The aIm component is the variable describing statement outcomes, actions or goals (Appendix H, Table 5). A Position rule is determined by whether the Aim verb is of the form "be". A Boundary rule is determined when the Aim verb suggests an action that allows an actor to "enter" or "leave" the action situation (Appendix H, Table 9).

A number of Position Rules found in the UGA data indicate the required participation of much of the leadership. The UGA observations show a number of observations coded as position rules specifying the participation of individuals from "Legal Affairs", "Bursar", "Human Resources", etc. By inference, these actors must be allowed to "enter" the respective action situations. Coding these Position rules required counting them as mandatory Boundary rules for the construction of the table showing TMS via participation of leadership (Table 6-11).

Requiring an observation to specify participation directly is also problematic. Georgia Southern has specific invite rules that do not mention "faculty", "Bursar", or "Extended Campuses" like UGA. However, interview data shows that the CIO and CISO make every effort to include all appropriate leadership in policy discussions. These observations are consistent with the design philosophy found in the rules structure of

the AGILE design method. So, while an observation specifying participation does not exist in the GS case, the rules-in-use indicate that a flexible rule for inclusion does permit participation, and in fact encourages participation.

A final observation, when you eliminate the observations from the documents created as part of the PCI supervised audit of security at UGA, the mandatory participation rules disappear. None of the "invite" boundary rules specify campus leadership at UGA. Given the issues discussed, I am unable to draw a conclusion regarding Hypothesis 5b although individual cases generally support the concept, with UGA being the sole exception.

6.2.2.3 Presence of Symmetric Aggregation indicates existence of collaborative culture

> **H5c**: The presence of symmetric Aggregation rules along with Open Boundary rules reflects existence of a collaborative culture and the governance structure is more likely to resemble a completed Knapp model.

A symmetric aggregation rule indicates a democratic process of achieving consensus. Symmetric implies relative equality among the actors for making decisions on outcomes. If these types of rules exists, then one expects the organization has a collaborative culture supporting the rule. Aggregation rules "determine the control an actor may exercise over the selection of an action" (E. Ostrom and Crawford 2005a, 191).

Observations coded as Aggregation rules are sorted by organization and ACUPA step (Appendix T). A scan shows a few observations inferring a consensus or majority of members required to approve a draft policy, such as found in Table 6-13.

Table 6-13 Example Symmetrical Aggregation Rules

ACUPA	A	I	B	C	Org	ref	Deontic
4.04	the president's cabinet	approve	draft policy	[at all times]	UGA	472 : 23	R
4.04	the University Senate (academic and Student Policies) or the Administrative Council (administrative policies)	approve	All university-wide policies	prior to final approval by the President, as set forth in University Statutes.	GSU	475 : 13	R

Document 472 is the Security Charter which UGA does not maintain as a set of current rules-in-use. Elimination of observations from this document brings the UGA decision action back to the structure employed prior to the Payment Card Industry audit. The UGA Network Security Standards, document 381, approved in 2005 and the Password policy, origins unclear but language consistent with 2001 versions found in other cases, place the sole decision-making authority with regards to a final policy version on the shoulders of the CISO and CIO [382:30, 381:29]. In a sense, the structure evolved from a non-symmetric Aggregation rule found in these statements (circa 2001-2004), to a democratic consensus found in the Security Charter created during the PCI audit (2008), back to a non-symmetric rule [471:15] (2011).

GSU Aggregation rules show a required consensus via observations found in the University Policy on University-Wide Policies [475]. But, we know that this process cannot be executed unless the Office of Legal Affairs approves the need for policy and the policy draft [470:6]. The sole exception is the requirement within the Network Standards policy [368]. This policy requires the Information Security Officer to work with stakeholders to develop standards, procedures, and guidelines – all necessary

policy components. But, no consensus is required to create policy as that condition is reserved to the Senate and Administrative Council.

Once again, I find that a single rule type does not meet the necessary and sufficient conditions to unilaterally affect structure. Other rule types contribute to the decision process.

Georgia Southern has formal rules in place that strongly suggest the CIO and CISO have broad, almost unilateral authority to make final decisions [336:46]. The Aggregation rules observed at Georgia provide the CIO with similar authority [343:184]. In both cases, other rule types create a decision structure that cannot move forward without some level of consensus. Georgia Southern specifically grants the Team authority to simplify a policy [473:9] prior to seeking feedback from the Technology Advisory Council [474:8] and informing Stakeholders [336:21]. Both the CIO and CISO are required to inform stakeholders and solicit their input [336:18-22]. Both positions are required to seek input from Legal Affairs [470:18], and Audits [470:9]. All of these actions are coded as Choice. The Georgia Tech process has both formal and informal rules requiring multiple levels of information exchange and feedback. For example, a rule coded as Information requires the GT Information Security Office to "vet the proposal" with the "faculty executive board, faculty senate, and all units of the campus" [476:4].

At UGA, the CISO refines the strategy for developing policy in consultation with team members [471:3]. The final decision to develop policy is defined by a Choice rule [UGA 471:13]. Per this observation, authority resides with the more ambiguous

Attribute “UGA”, implying that the cabinet, President, and IT team reach a consensus after reviewing all alternatives. Those alternatives are carefully considered because the “cost” of developing policy is the 18-24 months of effort required to create university policy. For that reason, an unwritten rule is found that forbids UGA from developing policy documents if those documents replicate policy mandated by an external entity such as the Board of Regents, the U.S. Congress, and the state legislature [471:16]. In sum, UGA defaults to referencing an external requirement. This decision does not require consensus of stakeholders.

Clearly, a true test of the premise of the hypothesis, should consider the effects of the configuration of rules, rather than relying upon a specific instance of a rule type. The “final approvals” rules are found in Step 4 “Get Approvals”. I eliminate the documents no longer in use at UGA [Security Charter] and GSU [University Policy on University-Wide Polices]. With this action, GSU presents zero observations in this step. The hypothesis suggests an Ad Hoc structure for GSU. UGA is left with rules from the Password policy document. Given no reference to other policy types, the hypothesis suggests UGA has a structure deficient in Knapp processes. Georgia Southern presents a configuration of Choice, Information and Scope rule types that suggests a rigorous feedback mechanism. In fact, the Scope rule requires that “Policy Owners must satisfy the stakeholders through timely and continuous policy actions” [473:1]. This statement comes from the AGILE document, but its intent is reflected in the number and the Aims of the statements from other policy documents. The hypothesis suggests Georgia Southern reflects a stronger version of the Knapp model than UGA or GSU. Georgia

Tech presents a number of Information rules requiring the exchange of policy drafts and feedback with stakeholders and Choice rules requiring approval by the Policy Review Committee, composed of many campus leaders, and the Cabinet. Again, the hypotheses suggests GT has reflects a stronger Knapp model. Hypothesis 5c is supported.

6.2.2.4 Presence of Information rules exchanging data among actors

> **H5d**: The presence of information rules requiring the exchange of information among actors indicates the existence of a collaborative culture and indicates a stronger governance structure when compared to cases without such rules.

An Information rule is determined by verbs indicating a "send or receive" function (E. Ostrom and Crawford 2005a, 191). I collected all observations coded as Information rules (Appendix U). UGA has one such observation [472:21]. The hypothesis suggests it is unlikely that UGA's governance structure will resemble the Knapp Model.

GSU has 22 such observations. A frequency analysis of Information Rules per Policy Document shows that 5 of the observations originate from the University Policy on University Wide Policies [475]. Three observations are sourced to the interview [470]. The remaining 14 come from the Information Security Management System Policy (ISMS) [367], a product of the limited implementation of the ISO 27002 security standard. The three statements found in the interview state that the CISO must present draft policy to Internal Audits, CIO, and the responsible Administrative council. Observations found in the ISMS document detail the types of information to be included in management reviews. Those management reviews include representation of

appropriate stakeholders. As this policy applies to only three divisions, the hypothesis, at best, indicates a partially recognizable Knapp model at GSU.

Georgia Southern Information rules outline what information should be distributed to whom and when. The rules are found in the IT Policy Development and Review Process document [336]. The hypothesis suggests GS will present a structure strongly resembling the Knapp model.

Finally, GT presents the strongest presentation of Information rules with 32 observations, accounting for almost half of the 76 metapolicy observations analyzed. The observations offer detailed direction as to what information is offered when to which groups. The hypotheses suggests GT governance structure more strongly resembles the Knapp model. Hypothesis 5d is supported.

6.2.3 Autonomy

> **H6**: If Scope rules limit actions of sub-units to modify policies, the governance structure is likely to resemble a Knapp model.

This hypothesis focuses on observations that restrain the sub-units of a case from amending or ignoring university policy. Scope rules define outcomes that must, must not, or may be affected by actions taken (Ostrom and Crawford 2005b, 208). Scope rules constrain the range of outcomes available (Ostrom and Crawford 2005b, 208). A scope rule may be used to affect an outcome otherwise not attainable using choice rules. I collected all observed Scope rules in Appendix V. The findings indicate support for the hypothesis.

There are no observations coded as Scope statements for GSU. The hypothesis indicates GSU governance structure will have deficiencies when compared to the Knapp model and other cases with such statements.

UGA explicitly restrains its departments from amending the password policy. Given that is the sole observation, the hypothesis indicates autonomy is strong and the governance structure at UGA will be deficient when compared to the Knapp model.

Autonomy is restrained under the GT Policy Review Process [360]. Scope rules make it clear that organizational units of GT (i.e. Campus units, GT Organizations) must not reduce the requirements established by this process [343:14]. The same units may augment [343:13] restrictions but at no time may campus units create rules that take precedence over policy created by the process [476:5]. Individuals from Information Security, Internal Audits, and the unit requesting the exception must review the proposals [353:16], gain the approval of top management for the request[353:17], and evaluate the request within given parameters [353:19-21]. The hypothesis suggests that the GT structure is likely to be formal.

The formal observation, found in the Acceptable Use Policy published by Georgia Southern [332] says the University must, at a minimum, comply with USG policy. A statement of scope pertaining to satisfying stakeholders may suggest a "tip-of-the hat" to a group's autonomy. But, a clarifying statement from the interview of the Georgia Southern CIO indicates that autonomous behaviors resulting in weakened university

policy is strongly discouraged[46]. Hypothesis indicates GS governance structure should strongly resemble Knapp.

6.3 Summary - How does the governance structure vary among the cases?

The chapter began by following a document level analysis of policy structure. That structure is hypothesized to reflect an appropriately formal level of governance structure. The tools of the IAD framework identified configurations of rules and actors that were thought to be present in Formal structures and weakly present in informal structures. Drilling down into the specific ACUPA tasks provided support for the notion that formality of structure is found in organizations with strong TMS and a culture of collaboration. The analysis of observations within ACUPA sets also confirmed that it is the "configuration of rules", rather than the presence of a single rule type, that is important to rigorous analysis of these structures.

External conditions clearly provided incentive for a change in governance. We have two cases, Georgia Tech and UGA, which experienced major breaches involving credit card data. GT responded to the coercive pressure brought to bear by the Payment Card Industry by restructuring governance of policy making and increasing the negative payoff for non-compliance by deans and department heads. UGA responded

[46] Interview indicates pro-active CIO works to "dissuade" departmental amendments. Can the departments or colleges do additional policy either more constrictive or as an amendment to your institutional policy.
Q: Can the departments or colleges do additional policy either more constrictive or as an amendment to your institutional policy. Answer:
Philosophically I would probably discourage them from doing something more or less. It doesn't occur and if it does, I'd try to reel it back in to what the institutional policy is. There may be some different procedures that are followed in various department or what not but I don't call those policy changes.

to similar coercive pressures by creating an executive level review committee and creating tight privacy policies to support explicit credit card policies required by PCI. However, UGA did not structurally change the way policy is made at the collective level and did not specify payoff incentives to encourage the type of collaboration that would ensure compliance. Georgia Tech did substantially change its governance structure.

Responding to multiple breaches, the governing body of the four cases, the University System of Georgia, revamped its rules outlining expectations that the cases should follow. Georgia Southern demonstrated a voluntary effort to comply with USG requirements. The Georgia Southern culture is one that rewards collaboration and consensus. Coercive pressure was not involved in policy changes.

Georgia State attempted to do what no other university in the world had done as it began a program to incrementally increment security standards promulgated by the International Standards Organization. However, a university governance structure did not adopt the standards promoted by ISO outside of two IT units and a financial unit. As a result, the governance structure at Georgia State resembles more of a weakly informal structure, perhaps even ad hoc like that of UGA.

The findings summarized in Table 6-14 show a pattern of support for the idea that policy structure will reflect the formality of governance structure and for the notion that organizational conditions, such as TMS and a collaborative culture, are “baked” into the institutions governing policy making. These findings suggest the “missing link” tying the performance of policy with the act of policy making (Robichau and Lynn Jr. 2009) may be observed in a robust and reliable manner.

Table 6-14 Summary Findings

Factor	Georgia Tech (GT)	Georgia Southern (GS)	Univ. of Georgia (UGA)	Georgia State (GSU)
Security Office	ISO – one person focused on security, additional personnel focused on compliance, monitoring, implementation	ISO one person, other responsibilities	ISO – one person focused on security, responsibilities for implementation and monitoring distributed across the organization	ISO –two persons, security officer and security engineer
Policy Structure	Formal	Informal (Strong)	Ad Hoc	Informal
Governance Structure	Formal	Informal	Ad Hoc	Informal/Ad Hoc
Metapolicy present	Yes	Yes	No	Limited to 3 departments
Knapp Model	All but Retirement	Weak retirement	No Retirement, weak awareness, risk assessment	No retirement, weak Risk Assessment
External Standard	ACUPA, NIST	AGILE	PCI (limited)	ISO 27002 (limited)
Culture: Autonomy	Budget controls/limits implementation	Autonomy not identified as a factor	Strong factor, bias to autonomy	Bias to autonomy
Culture: Collaboration	Provided by rule/norm	Norm driven supported by rule	Weak, when Top management requires	Weak, informal requirements in process
Culture: Top Mgt Support	Strong – compulsory	Strong – compulsory and cultural	Formally – strong; practice weak; affected by autonomy, budget	Weak
Hypothesis				
H1: The structure of a policy governance process will be reflected in the formality of the policy structure created by that process.	True	True	True	Not True –
H2: If an organization possesses a meta-policy then the likelihood that that organization observes most if not all of the processes	True	True	True – more deficient processes than GS/GT	True – more deficient processes than GS/GT

216

Table 6-14 (continued)

Factor	Georgia Tech (GT)	Georgia Southern (GS)	Univ. of Georgia (UGA)	Georgia State (GSU)
identified in the Knapp model is greater than an organization without a meta-policy				
H3: An effective formal governance structure presents a full complement of components and Knapp processes to be effective.	Not Clear	Not Clear	Not Clear	Not Clear
H4a: Governance structure will resemble the ideal Knapp model as the number of principals identified in 1st order boundary rules increase	Supported Data indicate a more formal relationship among actors and policy process institutions	Inconclusive Expectations are supported – informal process with relevant Top Management identified – yet need comparative case data to reach conclusion	Rejected Formally, the evolution of structure from near Ad Hoc to near formal network occurred when Top Management was named as participants in the Security documents required by PCI.	Supported No formal rules require top management participation; governance structure is deficient in the necessary Knapp processes for areas not under ISMS [367]
H4b: High TMS is likely accompanied by compulsory Boundary rules requiring the participation of a number of principals of the organization.	Supported GT presents compulsory and invitation rules. The number of principles engaged indicates relatively strong TMS and GT presents the Knapp model well	Supported The CIO does employ invitational boundary rules. And, the structure at GS represents the Knapp model well.	Supported Practice currently reveals the structure is deficient in necessary Knapp processes as the participation of top management is declining.	Supported CISO almost a "lone wolf" as she is only one focusing on security policy for an organization among the largest within USG
H4c: If there are no compulsory boundary rules, then the likelihood that a techno-centric governance process increases. TMS will be "lower" than in	Supported TMS is indicated within the process institutions	Inconclusive The measure of TMS is the representation of high level management in the policy process. But, there are no compulsory boundary rules found. Yet, indications are	Supported Directives from the Provost/President created compulsory rules as part of the compliance to USG and PCI demands. But these directives, instigated by PCI audit, are no	Supported GSU has low TMS. The only compulsory boundary rule requires the CIO/CISO as responsible for drafting policy. IT centric – suggesting ad hoc policy structure

Table 6-14 (continued)

Factor	Georgia Tech (GT)	Georgia Southern (GS)	Univ. of Georgia (UGA)	Georgia State (GSU)
organizations with compulsory boundary rules.		that by invitation TMS is achieved.	longer followed – no compulsory rules, weak TMS	
H5a: The presence of Open Boundary Rules setting the criteria for participation in making security policy reflects an organizational condition that values collaboration.	Supports Individuals may opt in, criteria for participation on committee also clear.	Supported Requires heavy reliance on rules-in-use. There is an informal open boundary allowing anyone to contribute to specification of needs or feedback to proposals.	Supported No open boundary rules identified, and the structure presents Knapp deficiencies.	Supported No open boundary rules found. Policy structure looks has Knapp deficiencies.
H5b: The absence of an invitation boundary rule specifying participation of university leadership will increase the likelihood of a governance structure that is largely ad hoc in nature.	Supported GT specifies TMS participation via a number of boundary rules. Structure resembles Knapp.	Supported GS has invitation boundary rules present. Structure resembles Knapp.	Not Supported Invitation boundary rules exist but use of rule in practice is not clear and there are Knapp deficiencies	Supported The only invitation rule is an administrative advisory committee with scope limited to examining the form of policy, not the content and the resemblance to Knapp is weaker than cases with such rules.
H5c: The presence of symmetric Aggregation rules along with Open Boundary rules reflects existence of a collaborative culture and the governance structure is more likely to resemble a completed Knapp model.	Supported – A configuration of information and choice rules support the notion that a collaborative structure is evident in the rules	Weakly Supported AGILE process supports symmetric choices. However, Formal rules lean toward non-symmetric aggregation rules permitting CIO/CISO to make final arbitration.	Supported A symmetric rule is not identified. And, the structure has weaknesses when compared to Knapp.	Supported A symmetric rule was not found. GSU structure is deficient when compared to Knapp.
H5d: The presence of information rules requiring the exchange	Supported GT specifies a number of channels to communicate	Supported Information rules requiring exchange are found in the	Supported This case has a lack of information rules and the	Supported The process of information exchange is mostly among

Table 6-14 (continued)

Factor	Georgia Tech (GT)	Georgia Southern (GS)	Univ. of Georgia (UGA)	Georgia State (GSU)
of information among actors indicates the existence of a collaborative culture and indicates a stronger governance structure when compared to cases without such rules.	with stakeholders during each stage of the process	informal and formal rules-in-use. .	structure has no retirement, very weak Risk Assessment and Awareness	the administrative leadership, and is informal (interview data). Governance Structure has weak resemblance to Knapp
H6: If Scope rules limit actions of sub-units to modify policies, the governance structure is likely to resemble a Knapp model.	True All but formal retirement process. It may be argued that the review process does act to retire policies.	Weak – no specific scope statement, but evidence that autonomy is managed within the formal process to prevent non-compliance by departments	True Autonomy exists –and the governance structure at UGA is not formal.	True No formal structure present – may explain the lack of structure for Retirement, and Risk Assessment

Chapter 7–Policy Structures

Effective policy is an outcome of effective policy governance. Simply having a policy will not prevent breaches of security (Neil F Doherty and Fulford 2005). Effective governance aligns policy with organizational structure (Pieters, Dimkov, and Pavlovic 2013), organizational environment (Sangseo Park, Ahmad, and Ruighaver 2010), and organizational culture (Baskerville 2006). Effective policy is operationalized by understanding these four elements: 1) whether the necessary components are present in the structure; 2) whether the scope of areas and issues covered is appropriate given organizational context; 3) whether the policy structure "fits" the organization; and, 4) whether the form of the policy content provides the clarity required for individuals to comprehend and integrate into operational decisions appropriately.

The previous chapter explored the structural details of policy governance and how the structure may vary as a consequence of varying organizational and external conditions. A theme of the hypotheses related to governance structure is that those conditions are "baked in". In other words, we find rules, standards, and norms that regulate policymaking for each case accommodating the pressures of the organizational culture, mission, external threats, and external mandates. This chapter explores the question as to the relationship between variations in governance structure and variations in the structure of the policy that is produced.

7.1 Relating Governance Structure to Policy Structure

Knapp's model (Figure 7-1) outlines four key processes necessary for effective security governance at the operational level: Awareness & Training, Implementation, Monitoring, and Enforcement.

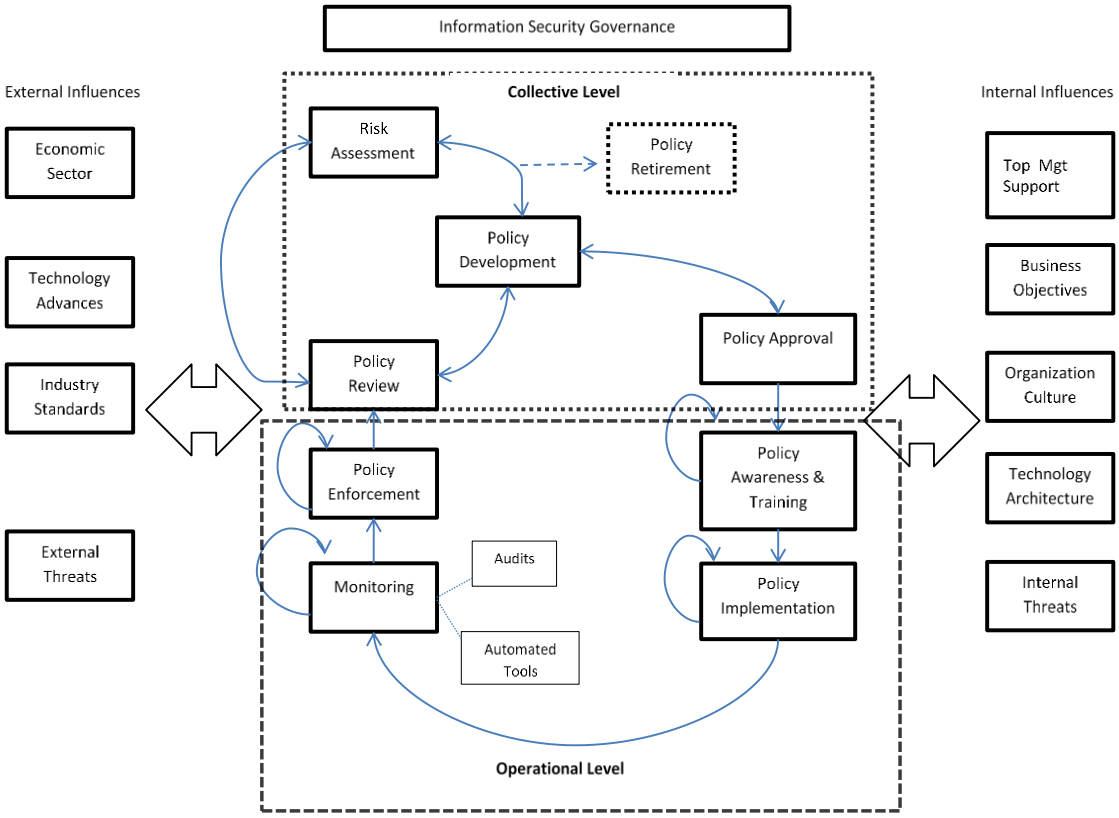

Figure 7-1 Knapp Model

Hypotheses explored in this chapter focus on the idea that the operational level policy structure is largely determined by the collective level structure. For example, an ad hoc policy structure – resembling small linear networks of a main document for each policy area with no links among the policy areas (i.e. password protection, data access) – is the likely outcome of an "it centric" governance structure – with little support from top management and little support from the culture of the organization.

As top management support improves, and collaboration improves – then the governance structure evolves to one that informally brings the major stakeholders together – the output of this governance structure is likely to approach an ideal network of policy actors and institutions, somewhat resembling a cluster, but with some gaps.

Finally, a formal governance structure increases the likelihood that the policy structure approaches the ideal model proposed by Knapp et al (2009). As the structure grows towards the complete Knapp model – the organization will invest the resources necessary to create the policy components required to ensure policy achieves expected outcomes. I apply this concept of structure to the data previously gathered (Table 7-1). The structure types identified range from Ad Hoc (UGA) to Formal (GT).

Table 7-1 Case Governance Structures - Descriptive Data

Factor	Georgia Tech (GT)	Georgia Southern (GS)	Univ. of Georgia (UGA)	Georgia State (GSU)
Organizational Conditions				
Size (Students enrolled)	19,431	19,150	33,367	30,606
Carnegie Class	RU/VH, DR	DRU, DR	RU/VH, DR	RU/VH, DR
Security Office	ISO – one person focused on security, additional personnel focused on compliance, monitoring, implementation	ISO one person, other responsibilities	ISO – one person focused on security, responsibilities for implementation and monitoring distributed across the organization	ISO –two persons, security officer and security engineer
Culture: Autonomy	Budget controls/limits implementation	Not a factor	Strong factor, bias to autonomy	Bias to autonomy
Culture: Collaboration	Provided by rule/norm	Norm driven supported by rule	Weak, when Top management requires	Weak, informal requirements in process
Culture: Top Mgt Support	Strong – compulsory	Strong – compulsory and cultural	Formally – strong; practice weak; affected by autonomy, budget	Weak
External Conditions				
Industry Standards	ACUPA, PCI	ACUPA, PCI	ACUPA, PCI, ISO 31000	ACUPA, ISO 27001/31000
External Threats	Credit Card Breach	Credit Card Breach	Credit Card Breach	None Reported
Governance Structure				
Knapp Model	All but Retirement	All but Weak Retirement	No retirement, weak Risk Assessment, Awareness	No retirement, weak Risk Assessment
MetaPolicy Present	Yes	Yes	No	No for organization, limited application of ISO to 3 departments
Gov Structure	Formal	Informal	Ad Hoc	Informal/Ad Hoc
Policy Structure	Formal	Informal (Strong)	Ad Hoc	Informal

7.2 Elements of Policy Structure

In Chapter 3, I discussed four elements of policy structure the literature found relevant to effective policy. Components of policy refers to the element of policy focused on the "pieces" of structure are present. Those components include instructions to create policy (metapolicy), manage policy (policy), implement policy (standards), and operationalize policy objectives (procedures and guidelines). Scope of policy details the problems and issues categorized as areas of focus or concern for policy makers. The "Fit" of policy measures whether and how well the policy is tailored to fit the unique organizational and environmental conditions. Finally, policy form measures the clarity of policy, in this case by its readability. The hypotheses regarding policy structure, discussed in chapter 3, are summarized in Table 7-2.

Table 7-2 Policy Structure Hypotheses

Hypothesis	Component Tested
H7: As an organization's governance structure declines from Formal to Ad Hoc, then it is less likely to present a coherent set of standards, procedures, guidelines and policies appropriate for effective policy.	Policy Structure - Components
H8: The likelihood of coverage of USG issues will correlate with the relative strength of top management support for securing cyber assets	Policy Structure - Scope
H9: Acceptable Use Policies will vary in "fit" as the governance structure varies. A Formal structure will provide greater evidence of fit, measured in terms of specific assignments and positions referencing that particular organization.	Policy Structure - Fit
H10: As the governance structure of a university becomes more formal, then the likelihood increases that clarity of the policy is more appropriate to the comprehension skills of the university's student population.	Policy Structure - Form

I confine my analysis of policy structure to one particular policy issue, Acceptable Use Policy (AUP) (Table 7-3). I do so for two reasons. First, the number of observations is more manageable (n=432). Second, external mandates create new requirements for

AUP documents in the 2008-2011 timeframe. This perspective provides "fresh" data to examine expected effects.

Table 7-3 AUP Operational Level Statements

Action.Situation	UGA	Ga Southern	GSU	GT	Row Total	Cell Contents
Awareness and Training	7	5	4	7	23	N
	0.33	0.21	0.01	0.00		Chi-square Contribution
	0.30	0.22	0.17	0.30	0.05	N / Row Total
	0.07	0.04	0.05	0.05		N / Col Total
	0.02	0.01	0.01	0.02		N / Table Total
----------	--------	----------	---------	---------	-------	
Enforcement	4	25	4	1	34	
	2.26	28.10	0.79	8.49		
	0.12	0.74	0.12	0.03	0.08	
	0.04	0.22	0.05	0.01		
	0.01	0.06	0.01	0.00		
----------	--------	----------	---------	---------	-------	
Implementation	95	83	55	115	348	
	1.08	1.00	1.17	0.71		
	0.27	0.24	0.16	0.33	0.81	
	0.90	0.72	0.70	0.87		
	0.22	0.19	0.13	0.27		
----------	--------	----------	---------	---------	-------	
Monitoring	0	2	16	9	27	
	6.62	3.74	24.79	0.07		
	0.00	0.07	0.59	0.33	0.06	
	0.00	0.02	0.20	0.07		
	0.00	0.00	0.04	0.02		
----------	--------	----------	---------	---------	-------	
Column Total	106	115	79	132	432	
	0.25	0.27	0.18	0.31		
----------	--------	--------	---------	---------	------	
Pearson's Chi2 = 79.36988**						
d. f. = 9						
P = 2.155744e-13						

The patterns identified in the analysis that follows show that the more structured cases, GT and GS, offer greater specificity in policy content. The two cases

also show the content reflects organization structure and conditions. UGA and GSU largely stay "ambiguous".

7.2.1 Components

Components are observed in the policy structure. My analysis of components and the network structure qualities of policy documents is where I tie together observations of the governance structure to observed qualities of the policy structure. In chapter three, I proposed one hypothesis concerning the relationship between the components of policy and the governance structure that produced the policies.

> **H7**: As an organization's governance structure declines from Formal to Ad Hoc, then it is less likely to present a coherent set of standards, procedures, guidelines and policies appropriate for effective policy.

I present a frequency analysis in Table 7-4. This is similar to the analysis found in Table 6-8 with two exceptions. This test focused only on AUP statements. And, the test focuses only on Operational Level action situations, so there are no metapolicy statements included. While the significance test suggests there is a relationship between the component observation counts and the cases, the pattern of that relationship is not clear. In the previous chapter, I concluded that this measure of structure for the entire policy structure is not sensitive enough to offer much explanatory power as to the nature of the relationship. For example, all four cases present similar distributions of procedural statements. There is no straightforward explanation by structure as to the frequencies of statements coded as procedures, guidelines, or policies. In sum, this hypothesis is not supported by the evidence presented.

Table 7-4 Distribution of Policy Components within AUP Operational Level Observations

Policy Type	UGA	Ga Southern	GSU	GT	Row Total	Cell Contents
Ancillary	1	0	0	0	1	N
	2.32	0.27	0.18	0.31		Chi**2 Contribution
	1.00	0.00	0.00	0.00	0.00	N / Row Total
	0.01	0.00	0.00	0.00		N / Col Total
	0.00	0.00	0.00	0.00		N / Table Total
Guideline	17	1	8	15	41	
	4.79	9.01	0.03	0.49		
	0.41	0.02	0.20	0.37	0.09	
	0.16	0.01	0.10	0.11		
	0.04	0.00	0.02	0.03		
Procedure	24	25	17	31	97	
	0.00	0.03	0.03	0.06		
	0.25	0.26	0.18	0.32	0.22	
	0.23	0.22	0.22	0.23		
	0.06	0.06	0.04	0.07		
Standard	55	59	36	41	191	
	1.41	1.31	0.03	5.16		
	0.29	0.31	0.19	0.21	0.44	
	0.52	0.51	0.46	0.31		
	0.13	0.14	0.08	0.09		
Policy	9	30	18	45	102	
	10.26	0.30	0.02	6.14		
	0.09	0.29	0.18	0.44	0.24	
	0.08	0.26	0.23	0.34		
	0.02	0.07	0.04	0.10		
Column Total	106	115	79	132	432	
	0.25	0.27	0.18	0.31		
Pearson's Chi-squared Test **Chi^2 = 42.15409** **d.f. = 12** **P = 3.13743e-05**						

7.2.2 Scope

H8: The likelihood of coverage of USG issues will correlate with the relative strength of top management support for securing cyber assets

Coverage of USG required policy areas was measured by identifying statements whose goals (aIm) were consistent with the objectives of protecting areas of concern

such as Password protection, data stewardship, and Acceptable Use. The findings are summarized in Table 7-5. The importance of proper coverage has been well documented in the literature. Intuitively, a well-structured policy process should produce coverage appropriate for the organization's conditions.

Table 7-5 Case Statements Per Requirement (Proportion)
(Legend: P-Present, W – Weakly Present, N- Not present; (% total statements)

Policy Area	UGA	GSU	GS	GT	Avg
AUP	W 0.24	W 0.23	P 0.30	P 0.41	0.29
Awareness	P 0.06	N 0	W 0.01	W 0.01	0.02
Copyright	W 0.01	W 0.02	P 0.07	W 0.01	0.03
Data Handling	W 0.12	W 0.03	P 0.19	P 0.29	0.15
Incident Management	W 0.01	P 0.03	N 0.09	W 0	0.03
Information Security Program	P 0.36	P 0.38	W 0.22	W 0.26	0.31
Password Protection	P 0.07	N 0	N 0	N 0	0.02
Privacy	P 0.14	W 0.01	N 0	W 0.01	0.04
HIPAA	N 0	N 0	N 0	N 0	0
Continuity	N 0	N 0	N 0	N 0	0
Cryptography	N 0	N 0	N 0	N 0	0
Electronic Data Disposal	N 0	N 0	P 0.03	N 0	0.01
Resource Mgt	N 0	P 0.28	P 0.09	N 0	0.09
Risk Mgt	N 0	P 0.01	N 0	N 0	0

The proportion of policy statements focused on an area is compared across the cases. A relative comparison uses the score of "N" if no statements are present, "W" if the proportion of statements is smaller than the average of the four cases, "P" if the

proportion of statements equals or exceeds the average. I record the results in Table 7-6. The coverage of Acceptable Use Policies shows the weaker structured cases with smaller numbers of statements. Only Georgia Southern exceeds the average with copyright protection. At the time of the study, GS was the only organization to include the protections that were mandated by the Higher Education Opportunity Act of 2009 passed by Congress to include copyright language that was demanded by the Recording and Motion Picture Industries.

Table 7-6 Summary of USG Requirements Met

Case	Present	Weakly Present	Not Present	TMS Strength
GT	2	5	7	Strong
GS	5	2	7	Present
GSU	4	4	6	Weak
UGA	4	4	6	Weak

The summary data does not indicate strong support for the hypotheses. To be fair, many of the USG requirements were set in policy long before the 2008 mandate. The AUP policy did undergo changes at each institution post 2008. The next two hypothesis will test the fit (tailoring) and form of the AUP policies that resulted from current governance.

7.2.3 Tailoring

Analysis focused on the AUP documents to determine if the statements in that document have been tailored to fit the organization.

> **H9**: Acceptable Use Policies will vary in "fit" as the governance structure varies. A Formal structure will provide greater evidence of fit, measured in terms of specific assignments and positions referencing that particular organization.

I discuss findings beginning with observations identified with awareness activities. The Implementation activities are subdivided to present information in practical groups defined by prior research.

7.2.3.1 Awa*r*eness

The observations are found in Appendix W. Table 7-7 presents a summary of the positions and the aIms (goals/objectives) for which an action choice by that position is expected GS refers specifically to its community with statements requiring their affirmation that their AUP agreement includes copyright compliance rules specified by the Higher Education Opportunity Act. GS requires "students, employees, and service providers" affirm their acquiescence to the AUP policy as they begin their relationship with the University and re-affirm as frequently as the CIO desires. GT delegates to the units responsibility for monitoring the compliance of their users with policy and for providing awareness session. GT also assigns responsibility to of Office of Information Technology (OIT) to provide support to those units for awareness activities. GSU focuses on older policies (Information System Ethics [365]: 2003; Minimum Security [368]: 2004) and places responsibility on users for consenting and understanding these policies. UGA places responsibility on the user community for maintaining awareness of AUP policies.

Table 7-7 Awareness - Fit of Positions and Issues

	Case	Generic Positions	Issue
Awareness	**GS**	Members of Georgia Southern Community Students, employees and Service Providers University CIO or designee	Acknowledge policy Publish policy
	GT	Unit Heads OIT Any person Unit faculty/staff University	Communicate awareness Facilitate awareness Provide training Compliance with AUP and Copyright
	GSU	Users University	Understand Password standards Follow Email rules Consent to monitoring
	UGA	UGA User Community UGA Student Body	Email Security Policy and Procedures

GS and GT make clear the positions responsible and reference organizational entities as such. In this regard, both cases link the policy to the organization structure as they reference policies (institutions) and positions. UGA refers to is user base in general terms. GSU does not name the university or any entity within the university. Neither UGA nor GSU reference awareness training activities organized by the organization. The relative strength of specific organizational references is consistent with the formality of governance structure. GT is the most specific with regards to organizational structure with GS relatively less so. GT shows a distributed network of awareness – delegating the monitoring, communication, and facilitation of awareness activities to the individual units. UGA is weakly represented and GSU the weakest.

The relationship between formal governance institutions that emphasize collaboration evidently contribute to the fit of awareness institutions within the organizational structure. GT formally requires participation of top management, and collaboration of unit management and other stakeholders, within the meta-policy titled

"Policy Review Process" [360]. GS documents similar requirements in its document entitled "IT Policy Development & Review Process" [336]. GSU has a document, "Information Management Security Policy" [367], that operates as meta-policy for three units only as resources prevented GSU from applying the ISO standard throughout the university. UGA has no single document defining meta-policy. Observations categorized from meta-policy are derived from a memo, "SecureGa Plan" [466], a charter, "UGA Security Committee Charter" [472], and interview data [471].

7.2.3.2 Implementation

Observations occupying the Implementation action situation are the most numerous. The observations were categorized using the AUP coverage criteria discussed in Chapter 3 (Table 7-8). I sorted the Implementation observations by AUP coverage by Organization and by Attribute (Appendix X).

Table 7-8 AUP Area Coverage Criteria

Issue	Definition
Access Management	Covers issues such as who is authorized to use systems and corporate information; username and password management regulations and good practice guidelines
Acceptable Behavior	covers permitted user activities, such as work-related use of the systems and information, and internet usage in particular.
Unacceptable behavior	Covers prohibited user activities, such as hacking, downloading illegal material, accessing illegal websites, dissemination of illegal or offensive material, sending bulk emails, harassment of other users, violating privacy of others users, dissemination of viruses, use of systems and/or corporate information commercial purposes, personal usage of systems and/or corporate information
License Compliance	Rules and regulations about software downloading, sharing and usage
Roles and Responsibilities	Explanation of the specific roles and responsibilities of users, system administrators, and so on
User Monitoring	Explanation of approach to monitoring user activities
Sanctions for policy violations	explanation of actions that will be taken in the event of a user breaching the acceptable use policy
Policy management	Details of responsibilities and procedures for policy management and maintenance

A scan of the results reveals patterns that conform to my expectation that as the governance structure grows more formal, so does the policy structure. For instance, the specificity in references to that specific case's positions, policies, and structures are higher for GT and GS and noticeably more ambiguous (i.e. university instead of Georgia State University) for GSU and UGA. UGA and GSU policy statements tend to be older. Older policy documents (created before 2005) that focused on password guidelines and acceptable behavior for use of university e-mail services are prevalent for the two cases with the less formal governance structures. As an example, I extract two AUP coverage areas: Acceptable Behavior (Table 7-9) and Access Management (Table 7-10).

Table 7-9 Acceptable Behavior

	Case	Positions	AIM and Object
Implementation Acceptable behavior	GS	Authorized users User	Act responsibly Connect to university networking Use IT resources only for intended purpose Do no harm Dispose according to procedures Abide by laws and USG policies
	GT	ResNet and Eastnet residents GT Community GT Employees users	Use assigned wired ports Use resources for scholarly purposes May use email lists Use resources in lawful manner Adhere to requirements for connectivity
	GSU	Individuals user Members of USG community	May join email lists Use secure web server Use GSU IT resources so privacy/access protected
	UGA	Users UGA E-mail users UGA user community UGA Student Body	May reference links and commercial sites Use ethical conduct Exercise caution when forwarding messages Practice acceptable use

GT specifically calls out policies and regulations from employee, student, and faculty manuals as it explains to differing groups of users how they may use IT resources. Both GT and GS are specific as to who grants access and monitors that access. GSU and UGA observations do not reference specific entities or titles when it comes to granting access. These two cases choose the more ambiguous university reference. Note that the AIMs for both UGA and GSU are more likely to reference an e-mail or password topic.

Table 7-10 Access Management

	Case	Positions	AIM and Object
Implementation Access Management	**GS**	GS University User Authorized user	Grant access (provide privileges) Requires Compliance to local, state, federal laws, GS policies Issue passwords According to authorization Use IT resources Must protect information
	GT	GT users	Provide resources Give accounts to all authorized GT users Check access privileges with managers Obtain permission from data stewards
	GSU	University users	Make resources available (to GSU students/employees) Use strong passwords Obtain/have valid authorization
	UGA	UGA Users No one	Allow use of email facilities for sanctioned activities Use for academic/authorized use only Use unique individual user id at all times May use without authorization

The licensing coverage highlights another age/detail difference (Table 7-11). Both GT and GS reference the need to respect copyright laws, a direct reference to the copyright mandates inserted into the U.S. Higher Education Opportunity Act (2009). The references for GSU and UGA come from policies not revised since 2005.

Table 7-11 Licensing

	Case	Positions	AIM and Object
Implementation Licensing	**GS**	GS University	Respect copyrights/intellectual property
		User Authorized user	Use in compliance with copyright and USG policy Cannot use resources without authorization form VP of Finance
	GT	GT	
		users	Must respect copyrights May not exceed licensed number of users for software
	GSU	University	Requires valid licenses for systems used by users
		Colleges and Operating Depts	Approve/retain documentation on software installed on department devices
		users	
	UGA	UGA	
		Users	May repost material using email only after receiving permission from the source May quote from source only if properly identified Reveal UGS information only after approved for release by appropriate office
		Computer users No one	Obey laws against private use of state property

The specificity inherent in the GT policy structure is demonstrated in the Policy Management area of the GT AUP policy structure (Table 7-12). Positions are given specific responsibilities. The units and unit heads are given latitude to monitor and

enforce, a deference to the distributed style of governance that GT stresses in its governance structure. GSU references some goals of general policy such as maintaining user confidence in the reliability of the systems and data made available. UGA observations focus only on e-mail policy created prior to 2004.

Table 7-12 Policy Management

	Case	Positions	AIM and Object
Implementation Policy Management	**GS**		
	GT	GT	Policy applies to all GT users Reviews requests for sites not ending in "Gatech.edu" Recognizes needs for policy exceptions
		OIT	Responsible for managing GT resources Delegate to specific units network admin responsibilities
		Units (Unit heads)	Provide centralized IT services Delegate network monitoring Maintain adequate tech support team Ensure sufficient funding for unit IT infrastructure
		Operators of NAT, DHCP, VPN	Delegate responsibility for IT planning Track and identify traffic by generated by individuals
		Technical leads	
		Users	Consider state of technology when evaluating tech for planning purposes Require authorization Must use policy exception process to share accounts
	GSU	University	Applies policies to students, employees Grants access of level required to perform job Provides site-wide license for anti-virus software to all Seeks to preserve individual privacy Maintains quality computing environment
	UGA	UGA	Committed to responsible use of information Applies email policy to all services owned by UGA Applies email policy to all users Applies email policy to printed emails Encourages academic and business use of email
		Appropriate university administrative office IT staff	Submit official approval of bulk email

7.2.3.3 Monitoring

GSU breaks its pattern of ambiguous Attributes and policy references with a marked increase in specificity. Most of the GSU observations are found in the System Ethics Document [365] last revised in 2003. GSU System Use Policy [361] says users "should" report violations. The e-mail policy [363] gives responsibility for monitoring compliance with e-mail standards to departments. And, the Minimum System Security Environment Policy [368] gives users responsibility for ensuring their PC is secure. The majority of GSU observations stipulate the generic "university" "may" "access and monitor" systems and system usage. The only required action of the university is the observation requiring notification of the user if the university must monitor activities on the user's account.

The number of GSU observations is in stark contrast to GS as it provides succinct direction to users and how they may or should report violations. Unlike GSU, GS requires users to report any observed violations. GT continues its delegation of authority to IT technical leaders and unit heads to observe and maintain compliance. GT users should report violations, but are not required. GT officials, on the other hand, must report violations and have permission to access and observe user accounts at any time. UGA monitoring requirements are limited to compliance with the e-mail policy [379].

While GSU presents the greatest number of institutional statements, the deontic is strongly biased to the "permissive", leaving decisions to monitor and report violations

to the individual or department. GT and GS show a stricter "must" deontic, requiring all to report known violations.

7.2.3.4 Enforcement/Sanctions

GS provides a significant and specific set of observations to enforce policy. The statements specify how the policies are to be enforced and who has latitude to determine the sanction applied. GSU specifies that sanctions will be determined by the appropriate judicial organization (student, staff, faculty) as prescribe by the handbook appropriate for the offender. GT offers a generic "violators will be prosecuted". UGA refers disciplinary matters to appropriate authorities, staying consistent with the philosophy of linking to external policies when appropriate. The relationship between governance and policy structures is not clearly defined for these actions. However, the actions are relatively weak when measured in terms of number of observations. The small n constrains the conclusions that may be taken from this step.

7.2.3.5 Measuring Indicators of Fit

A stronger presentation of the patterns discerned from Appendix X is created by counting the number of positions, aims, and conditions that met the criteria for specific references and those observations that used ambiguous references to "university", indicating a statement that could be "cut and pasted" into any college policy document. The results are shown in Table 7-13.

Table 7-13 Fitness Test

		GT				GS				GSU				UGA			
Issue	**Definition**	**Pos**	**Aims**	**Cond**	**# Obs**	**Pos**	**Aims**	**Cond**	**# Obs**	**Pos**	**Aims**	**Cond**	**# Obs**	**Pos**	**Aims**	**Cond**	**# Obs**
Access Management	Covers issues such as who is authorized to use systems and corporate information; username and password management regulations and good practice guidelines	2,0	0	3,0	6	4,0	0,1	2,1	9	0	2,2	0,3	5	0	0,3	1,0	5
Acceptable Behavior	covers permitted user activities, such as work-related use of the systems and information, and internet usage in particular.	4,0	2,0	4,0	9	0,3	0	0,1	8	0	1,0	0,1	5	3,0	1,0	1,0	11
Unacceptable behavior	Covers prohibited user activities, such as hacking, downloading illegal material, accessing illegal websites, dissemination of illegal or offensive material, sending bulk emails, harassment of other users, violating privacy of others users, dissemination of viruses, use of systems and/or corporate information commercial purposes, personal usage of systems and/or corporate information	3,0	7,0	4,0	25	0	1,7	3,7	32	1,0	0,1	0,3	18	0	1,3	2,4	20
License Compliance	Rules and regulations about software downloading, sharing and usage	1,0	0	0	4	1,0	0,2	2,1	5	1,0	0	0	2	6,0	2,0	0,2	7
Roles and Responsibilities	Explanation of the specific roles and responsibilities of users, system administrators, and so on	33,0	8,0	17,0	49	8,4	3,2	1,5	23	2,0	1,0	1,3	14	1,4	1,1	0,2	19
User Monitoring	Explanation of approach to monitoring user activities	6,0	3,0	4,0	13	0	0	2,1	5	6,9	0	1,5	19	0	3,0	0	3
Sanctions for policy violations	explanation of actions that will be taken in the event of a user breaching the acceptable use policy	0	0	0	1	12,7	3,4	8,6	28	0,3	0	2,1	5	1,1	1,0	1,0	4
Policy management	Details of responsibilities and procedures for policy management and maintenance	12,0	2,0	10,0	18	NA	NA	0		0,3	0	2,0	7	2,2	1,1	3,4	15
Criteria																	
Positions (Attributes)	Organizational specific and reference organizational structure			Key - (Specific, Vague): A reading of (8,4) should be read as follows. 8 observations referred to a specific title, position, policy, or department by name. 4 observations used a generic reference like "university".													
Aims and Object	Reference organization specific objectives																
Conditions	Reference organization and structure specifically - including named policies, divisions, goals																
	(in sum, looking language that does not apply generally to most organizations)																

The relative differences between GT and GSU/UGA are apparent. The count of observations for "Roles and Responsibilities" show the detail presented for GT in Appendix X. The number of times that a GT observation refers to the university or department within the Attribute by its appropriate name is a strong 33 out of 49 observations. GSU identifies itself 2 out of 14 times. UGA identifies only once. GS is relatively stronger with 8 identifications. The pattern supports the thesis that as the governance structure grows more formal, the specificity within the policy structure is more direct.

7.2.4 Form

This test uses the Flesch readability algorithm to measure the readability of the document. An Ad Hoc structure will produce lower reading ease scores, a Formal structure will produce scores closer to the reading level of the population that must understand and implement the operational level statements. A Formal structure will also present higher reading ease scores. The results of the test are shown in Table 7-14.

> **H10:** As the governance structure of a university becomes more formal, then the likelihood increases that clarity of the policy is more appropriate to the comprehension skills of the university's student population.

Table 7-14 Form of AUP Policy

Case	Flesch-Kincaid	Flesch Reading Ease	Length (# Words)	Date last revised
GS – AUP	12.3	19.1	2588	2010
GT AUP	14.6	26.9	4233	2011
GSU – System Ethics (AUP) [365]	16.5	14.4	852	2003
UGA – AUP [377]	12.1	19.8	1273	2004

A reading ease score that approaches zero increases in difficulty and decreases in clarity. While GT is close to 30, its text is still within the "Hard to read" category. GSU has the lowest reading ease score. But, GS and UGA show similar scores that are not much better than GSU. The findings of this hypothesis are mixed at best and do not clearly support the premise with demonstrable clarity.

7.3 Summary

This chapter explored findings related to hypotheses testing the relationship between governance structure and policy structure. In particular, I examined four elements of policy structure that prior research suggests are essential elements of an effective policy. The hypotheses express the expectation that a more formal, and thus more effective, governance structure should produce relatively a more effective policy structure than an ad hoc, and less effective, governance structure. I summarize those findings in Table 7-15.

Table 7-15 Findings Summary

Hypothesis	Element Tested	Conclusion
H7: As an organization's governance structure declines from Formal to Ad Hoc, then it is less likely to present a coherent set of standards, procedures, guidelines and policies appropriate for effective policy.	Components	**Not Supported** Count data of component statements not sufficient to explain the structure.
H8: The likelihood of coverage of USG issues will correlate with the relative strength of top management support for securing cyber assets	Scope	**Not Supported** Test of data may not be precise enough to measure relationship
H9: Acceptable Use Policies will vary in "fit" as the governance structure varies. A Formal structure will provide greater evidence of fit, measured in terms of specific assignments and positions referencing that particular organization.	Fit	**Supported** Precision greatly enhanced with use of institutional analysis tools – grammar and rule configurations
H10: As the governance structure of a university becomes more formal, then the likelihood increases that clarity of the policy is more appropriate to the comprehension skills of the university's student population.	Form	**Not Supported** Results are mixed.

The failure of Hypothesis 7 cannot be taken as the final finding regarding the relationship between governance structure and the composition of effective policy. The test examines only one dimension of structure, institutions. Ostrom defined structure as one that is defined by the set of actors and the rules that regulate their actions (E. Ostrom 2005). One could propose a test where you compare the composition of components in other policy areas apart from cybersecurity for the same organization. Actually, a test of the average composition of a significant number of policy areas would provide a grounded approach for analysis of this relationship.

While one can expect that a strong governance structure will produce necessary and sufficient coverage of policy issues, the test used for Hypothesis 8 is not a precise one. How many institutions does it take to cover the issues within a particular policy

problem related to the organization's context? The measure used may suffer from an ecological fallacy. Is the association of the proportion of observations categorized by policy area related to the compositional effectiveness of the policy? Would an analysis of rule configurations within each required policy area provide a more cogent measure of compliance? What does an ideal proportion of institutional statements per policy area look like?

As to effectiveness, copying and publishing a policy does not necessarily affect the rules-in-use. And, it is the rules-in-use that genuinely defines the structure of an action situation. "Paper Tigers" are a well-known means of meeting compliance measures that yield outcomes that fall short of expectations. However, no observations means no policy. And, no policy is not effective policy. More work to be done in this regard.

Hypothesis 9 provides the strongest test of linking the outcomes of varying degrees of formality of governance structure with the necessary elements of effective policy structure. Analysis of rule types and the construction of those rules via the value found in the statement components, particularly the Attributes, aIms, and Conditions; provide data that offer cogent descriptions of the differences in structure between Ad Hoc cases, such as UGA, and Formal cases, such as GT. I believe further research will confirm this finding and expand the possibilities of relating policy content and structure to organizational conditions.

Finally, the failure of the hypothesis test for policy form cannot be an indictment of the concept. Rather, the test should be revised to include data from surveys of users, managers, and other groups of actors as they interpret the policies.

A failure of the design used for these tests is the decision to focus on Acceptable Use Policy as the only policy area. A more robust test would explore how all areas with written policies are structured and whether those areas share components and processes as appropriate. The success of using IGT tools to "dig deeper" into the structural analysis holds promise, especially as it relates to increasing the precision of analysis by aggregating multiple institutional statements as units of observation. The method needs much refinement, but the general findings of this chapter do encourage further exploration of the relationship between the collective and operational action situations, and the use of IGT tools to measure the differences of those situations.

Chapter 8– Discussion

Are there patterns, trends, and other generalizations identified in the previous three chapters that indicate the study's objectives were achieved? Do those findings agree with research in the fields identified? I begin by summarizing the research framework and study design. The findings are then discussed in the context of the hypotheses posed in Chapter 3. I summarize the discussion in the context of the research objectives and more current applications of the IAD tools to understand municipal, regulatory, and organizational policy designs.

8.1 Purpose of the Study

My research question is motivated by a personal curiosity developed while serving as deputy to the CIO of the University System of Georgia. The governing board of the USG prescribed a path for the individual units to follow in order to develop information security programs. While tremendous freedom was given to the units to tailor those policies, the variations of responses were not uniform. The responses varied within groups of USG units of similar size, mission, and resources. From my observations, the following question emerged: "How does Policy Structure vary as a function of Policy Governance?"

The literature documents the variation in scope and structure of security policy in sectors such as postsecondary education. Findings in the literature suggest that if we are to develop and implement effective cyber security policy then we must have effective policy governance. Policy governance is the interaction of actors whose

decisions are regulated by institutions as they work together to create policy. Policy structure is how an organization's work to manage organizational behavior is organized (Robichau and Lynn Jr. 2009). It is this interaction that determines the policy structure of an organization (Arnold and Fleischman 2013). In this study, policy structure is conceptualized as a configuration of the statements that compose the strategies, norms, and rules use to govern the behaviors of actors and organizational entities. Theoreticians care about policy structure because that structure determines the outcomes and outputs that determine the effectiveness and efficiency of policy, the determinants of how and whether policy works. Practitioners care about policy structure because that structure determines how efficient and effective the security solutions are, and whether the organization's strategies, objectives and mission are protected.

A review of the cyber security research literature found no integrative framework to describe, much less predict, how organizations adopt and implement cyber security policy (Hsu, Lee, and Straub 2012). In other words, a robust method to identify the key features of an organization's policy governance structure was lacking. In order to answer my question, I integrated concepts from institutional analysis, information security, policy governance, and policy implementation into a research framework described in chapter 3. The tools of analysis were adopted from the Institutional Analysis and Development Framework. The security governance framework developed by Knapp et al. (2009) fit easily into the IAD framework thus

providing a model recognizing the various contextual factors and the interaction of context with structure.

The integration of institutional analysis theory with security theory is not new. But, the application of the tools previously used to analyze governance structure of "problems of the commons" is unique. I used the institutional grammar tool and analysis of rules configurations to identify and map features of structure essential to effective policy. Measures of relative strength of structure were developed to aid in the cross-case comparison of these structural features.

The framework suggested a number of hypotheses, guided by both institutional and information security theory, to test the relationship between governance structure and the various policy structures found within the USG units. Scarce resources for a study such as this naturally limited the number of external and organizational factors the effects of which could be considered in this analysis. I focused on mandates from external sources such as the Board of Regents and the Payment Cards Industry as motivators to structural and policy changes among the cases. I also chose to focus on the concepts of Top Management Support and the cultural values of collaboration and autonomy as primary factors from the organizational conditions.

The case study method was chosen as my research context involved questions of how and why within a set of events that I did not control (Yin 2009). I chose to examine 4 cases involving USG units with similar missions as research universities. Those cases provided paired observations of similar size (UGA & GSU, Ga Sou & GT), similar resources (UGA & GT, Ga Sou & GSU), and similar external conditions (UGA &GT –

breaches, GSU & Ga Sou – no breach). Data was collected from multiple sources. I inventoried and catalogued the policy documents using the methods described by Doherty, et al (2009). Those documents were then analyzed using the Institutional Grammar Tool to decompose the observations. Interviews of the primary actors, usually the CIO or CISO, for each case provided insight as to informal policies and institutions. The transcripts of those interviews were coded in the same fashion as policy documents. The configuration of rule types were then collected into the action situations defined by Knapp, as well as those defined by the ACUPA model. The ACUPA model permitted more discrete analysis on situations with specific expectations of outcomes such as team selection, draft revision, etc. From these analytical exercises, several findings emerged.

8.2 Summary of Findings

Findings suggest a direct relationship between structural features of policy governance (i.e. the actors and institutions configured to develop policy) and the structure of policy produced by that process. A cross-case comparison of policy governance identified key features that explain those differences. Prior research suggests that these differences are predictive of effectiveness of policies for the respective cases.

The key features identified are:

- UGA institutionalized the reference to external policy mandates as preferable to managing a policy review and development process to adapt mandates to fit organizational conditions.
- GSU institutionalized a critical “go/no go” review by the Office of Legal Affairs.

- GSU's governance structure is "bi-furcated" – three departments employ the ISO 27002 standard, the remaining departments reside under a structure described by the "University Policy for University-Wide Policies".
- GS institutionalized a system design philosophy (AGILE) that emphasizes a "bottom-up" style of policy development. However, the scope of this method remains under the tight control of the CIO.
- GT features the largest divergence from the models suggested by the University System and external standards organization. Yet, the governance structure provides a collaborative method to tailor policy to fit various and divergent organizational conditions found within the larger enterprise of the university as a whole.

These features were found to relate to differences in the strength of the formality of the respective governance structures. Analysis of the presence and relative strength of structure of the Knapp action situations, along with identification of whether a metapolicy is present, contributed to a sliding scale of formality of structure. GT was identified as the most formal, followed by GS. UGA and GSU both were tagged as possessing a structure with Ad Hoc features, but GSU, largely due to the limited implementation of the ISO 27001 standard, was noted for an "informal" governance structure. The criteria for evaluating policy structure found similar assessments, confirming the primary hypothesis that formality of policy structure is defined by formality of governance structure.

Before discussing findings specific to the hypotheses tested, a few general observations must be discussed. This study affirms the need for avoiding the reification, or in some cases "deification", of institutions. Individuals may or may not share mutual expectations of an action situation, the intent of its institutions, even the comprehension of the information presented to affect a collective decision (Crawford and Ostrom 1995). In other words, institutions do not exist separate from those

individual and mutual understandings. The weak relationships found between the existence of specific configurations of rules and policy outcomes is a testament to that observation. Simply counting rule types is not sufficient. There must be a means of understanding how those rule types vary in terms of the actors identified and the conditions and objectives of the institutional statements as understood by those actors.

The literature affirms that policy must be aligned with organizational goals if the policy is to be effective in producing the desired outcomes. Simon proposed that the term "organizational goal" refers to the constraints imposed by the role that an individual plays within the organization. And, that decision-making (i.e. policy making) is a decentralized structure involving different sets of constraints for disparate organizational parts that affect decisions in other parts (1964). So, just as Crawford and Ostrom cautioned against reifying particular sets of institutions at the harm of ignoring the truth that decisions are outcomes of individual interactions, one must not reify the organizational goal and set it apart from a general understanding that goals are "fuzzy" perceptions within the limits of mutually shared perceptions of those goals. Given these cautions, the scale of structure formality employed in this analysis perhaps sets an appropriate expectation as to the precision of predicting policy structures and outcomes.

Monitoring and enforcement matters. The cases are compliant with a majority of the requirements within the USG policies and guidelines. However, their individual governance structures did not represent a mimetic implementation of those influences. The enforcement of standards created by the Payment Card Industry at UGA and GT was

a result of significant breaches of credit card data at those units. At GT, the enforcement action created a more centralized governance structure, and constrained the influences of autonomy while encouraging collaboration. However, at UGA, despite initial documents prescribing a centralized policy review process with cabinet-level participation, the process is not used. So, at GT, Top Management Support of formal and informal security policies is more easily observed and measured as a result of those enforcement actions. At UGA, the informal policies have sidelined the formal policies requiring such participation. While collaboration is documented and required at GT within a formal meta-policy, the energy required to create similar collaborative efforts at UGA is deemed too costly in terms of time and resources. The structure for such efforts at UGA are found in a memorandum but were not produced in a formal policy document.

Relatively weak Top Management Support, along with strong values of autonomy and mixed support of collaboration are noted within the action situations mapped for GSU. While Georgia Southern did not experience a traumatic external condition like a breach, the influence of the AGILE philosophy is found within those observations. The level of information rules, frequency of feedback, and sense of urgency yield policy outcomes that included a shorter time of development (4-6 months compare to up to 2 years), and a culture that is aware of the import of security issues exhibited by collaborative efforts not seen at GSU.

Internal conditions clearly affect policy structure. I found that the governance structure for information security policy making generally follows a standard such as ISO

27001, ACUPA, AGILE, etc. And those standards were largely selected on a couple of criteria : 1) The CIO's preferences based on information related to their experience and knowledge, and 2) whether the IT governance area was strongly integrated with the governance structure of the unit.

The diffusion of decision-making power reflects, and may be a proxy for, values such as autonomy and collaboration. At Georgia Tech, the enforcement action taken by PCI representatives formalized tighter controls by individuals held accountable by the entire organization for security outcomes. Accountability also flowed down through the organizational structure for successful implementation of those policies. Finally, top management required more information on a more frequent basis from all units of the organization as to policy performance. The diffuse structure at GSU reflects a lack of accountability within the rules and information flow across the organization.

I am confident that some elements important to assessing structure were not found due to weaknesses in the research design. A richer set of interview data, perhaps supplemented with sample survey data from the case populations would provide evidence of missing structural components. Counting observations coded for Knapp processes is not a strong quantitative definition of structure. Using comparisons of those counts (i.e.% of total statements compared to average) is a relativistic measure at best (see Table 6-5). But, at least it is a start.

The answer to my research question is in the affirmative. I did find a diverse set of institutions that describe the governance of policy-making within each case. I also found a correlation between organizational and environmental conditions and those

institutions. Perhaps most important, I found that the research framework, once modified with the ACUPA steps, aided the organization and interpretation of data significantly. The framework provided structure that made the task of analysis and follow-up easier to manage. In the following sections, I discuss findings specific to the hypotheses proposed in chapter three.

8.2.1 Structure

Measuring structure is an interesting exercise. I chose a continuous scale of structure that mimics the graphing of social networks to a certain degree. An ad hoc network is one resembling "loose" connections of seemingly disparate topics. A formal network shows connections between policy components (vertical connections) and policy issues (horizontal connections). An informal structure lies in between the two. Given the wealth of literature regarding policies and policy networks, it seems appropriate that defining policy structure could also benefit from what has been developed by the social network analysis literature.

The policy document was initially identified as the unit of observation used to map the graphs. The precision of this analysis, while thought provoking, is not robust in its representation of the true relationships among components (procedures, guidelines, standards, etc.) and the policy areas that those components are designed to regulate.

The second hypothesis simply tested how the presence of a metapolicy is reflected in the structure of policy governance. I created a relative measure of strength relating the presence of Knapp processes to the formality of structure and the presence of a metapolicy. The support of the hypothesis is validated to a limited degree.

Aggregating the policy statements, essentially creating count data, is not a precise description of the structure of those processes. Structure, as a concept, reflects the outcomes of repeated interactions of actors constrained by a given set of rules.

I propose digging further into developing a means of measuring the "strength" of individual Knapp processes in the future. Can the idea of "deficiencies", features essential to effective policy that are either missing or weak, be a predictor of policy outcomes. How can deficiencies be reliably identified and measured? Are there patterns within rule configurations that mark or predict the presence of deficiencies? These are but a few questions worthy of exploration.

8.2.1.1 Governance Structure

The study mapped key governance features against the ACUPA suggested model and found differences in structures that support the notion that differences of observed policy structures among the cases are related (Hypothesis 1). The findings affirmed that, as Baskerville and Siponen thought, the existence of a metapolicy predicts a more formal structure (2002). The GSU case demonstrated the need to be cautious in accepting the existence of a formal metapolicy as an indication that the metapolicy was institutionalized within the organization's governance structure. The GSU case also demonstrated the importance of identifying key features of governance, such as the review by Office of Legal Affairs. Such features can "short-circuit" the best designed processes, even those that emulate best practices or strong standards.

I shifted the focus to individual policy statements as the unit of observation. A chi-square analysis suggests a relationship between the cases and the distribution of

component types in the size and direction that is expected. The presence of appropriate policy components as indicators of policy effectiveness is one that has strong support in the literature (Baskerville and Dhillon 2008; Neil Francis Doherty, Anastasakis, and Fulford 2011; Moule and Giavara 1995; Baskerville and Siponen 2002). Measuring those combinations and proportions is an area of future research that this study indicates may have promise. Both theory and practice can benefit from understanding how those proportions may change per organizational context and how those proportions relate to measured outcomes of policy effectiveness.

However, the findings from the analysis of the set of hypotheses (3 a, b, c) that test this relationship do not strongly support the concept just described. Intuitively, one may expect that a more formal governance process would invest in the knowledge and process to sufficiently construct the necessary standards, guidelines and procedures to assure policy success. So, while the findings do not positively support this conjecture, I conclude that the study design needs additional thought before arguing that prior research is at fault. The ratios of observations for the components identified for each case do suggest a relationship between the composition of components observed and the cases. However, the details hidden within these component counts offer an opportunity to explore exactly what elements are related to the case conditions, and what elements are not. The tables and analysis produced by mapping institutions to the ACUPA model suggests deeper analysis of the variations of specific attributes, aims, and conditions of the coded observations may provide better answers.

8.2.1.2 Structure and Graphs – an exception

Structure did not behave as expected for the GSU case. Perhaps the limited implementation of ISO 27002, and the generic University Policy on University-wide Policies, cause the two structures to differ. The graphs suggest the documents and their references are artifacts of the "ad hoc" fashion of developing security policy. GS and UGA show the older policies of data handling, password protection, etc. that operate as though other policies do not exist. Later policy efforts "loosely" connected these policies together to form a system. GT's process demonstrates how developing a new policy process brings structure to the document relationships. Given the relative "newness" of the meta-policy, one can speculate that as time passes, the structure will exhibit more of the horizontal cross-references that a meta-policy is thought to encourage.

8.2.2 External Conditions

At the beginning of the study, I anticipated a finding that would show key features of externally mandated standards become part of the case policy structure. Georgia Southern and Georgia Tech both showed "copyright" features required from the federal Higher Education Opportunity Act. UGA and GT both showed features from the PCI standards to secure credit card transaction data. And, all four cases showed some affinity for the ACUPA model of policy governance.

The variation in compliance with USG requirements showed "independence" from the parent governing body as to the structure of security policy. Top management actors from each case, as well as the other units of the USG, participated in the

construction of these requirements. One may consider it odd that compliance varied as much given the participation. One plausible explanation is found in the evolution of USG policy requirements. From one year to the next, differing external standards were suggested by the USG Office of Information Security as the model to follow (e.g. NIST 800, ISO 27001, etc.). At one point, multiple models, some with fairly distinct differences in objectives, were listed as "ok" for units to adapt. The lack of firm guidance certainly would lower perceived risk of "non-compliance" among the case actors. A further note, the limited implementation of ISO 27001 at GSU was initially view with skepticism by USG personnel. Once outside praise of the implementation began to appear, the standard was added to the USG list.

Consideration for future research includes examining the processes that "filtered" these features and adapted them to the case organizational conditions. Initial observations suggest that a few key actors hold the power to filter and adapt the externally required features in a manner that reflects organizational priorities such as resource allocation, autonomy, and management objectives.

External mandates may instigate changes to governance and policy structure. But, those changes may not necessarily be "institutionalized", or integrated, into the fabric of organizational culture and operations. As the UGA and GSU cases confirm, a written rule does not mean the rule plays any part in influencing the discussion. UGA and GT experienced egregious breaches involving credit card data. Both institutions were subjected to severe penalties by the Payment Card Industry and were required to implement new policies that met PCI standards so that the organizations could continue

to operate as a merchant using those payment systems. GT chose to restructure policy governance and to institutionalize those standards along with other best practices to create a robust governance structure driven by the type of meta-policy suggested by Baskerville and Siponen (2002). UGA adopted specific documents in response to PCI standards, but operates under a system of "referencing" mandates within existing policy rather than engaging the campus community in a university policy process. The findings among the cases showed that despite similar external conditions, the two cases present different policy structures as a result of differing governance structures.

8.2.3 Organizational Conditions

I examined two sets of hypotheses that explore the relationship between governance structure and the organizational conditions related to Top Management Support and Collaboration. The findings supported the findings of earlier research, confirming the relationship and the direction of the relationship (Table 8-1).

8.2.3.1 TMS

Knapp et al (2009) found strong support for their proposition that "…an organization's overall security health can be accurately predicted by asking a single question: 'Does top management visibly and actively support the organization's information security program?'". I proposed a set of hypotheses to test this finding by approaching the analysis from the institutional perspective. The hypotheses propose that the presence of top management support can be validated and identified within the institutions that govern policy process and within the content of policy as well.

The findings affirmed prior warnings that rules-in-form (i.e. policy documents) are not sufficient proof. The identification of TMS in "rules-in-use" was more informative as to the role and extent of TMS within each case. The relative strength of TMS, measured in terms of compulsory boundary rules showed that the more formally structured participation of top management in the GT case yielded a diverse participation of actors reflective of the decentralized structure of the GT organization. The philosophy of AGILE similarly guided GS to be more inclusive than was the finding for UGA or GSU. As the inclusiveness of various top management from across the organization diminished, a more techno-centric oriented set of actors emerged at GSU and UGA. And, consistent with prior findings regarding the technical nature of information security policy and weak TMS, the two less formal cases presented the weakest security governance structures.

Perhaps the most significant finding is the correlation between the appearance, and frequency, of compulsory boundary rules and the strength of the formal governance structure. Rationally, given the perspective of most individuals, management or otherwise, that security is a technical issue, then certain actors must be compelled to participate. But, the use of a rule type, and in this case, a further refinement of that type, to identify a feature like top management support, suggests the methods provided by the IAD framework can be applied by policy analysts to sift through both rules-in-form and rules-in-use to identify potential deficiencies in effective structure.

Table 8-1 Hypotheses Exploring TMS and Collaboration

Factor	Georgia Tech (GT)	Georgia Southern (GS)	Univ. of Georgia (UGA)	Georgia State (GSU)
H4a: Governance structure will resemble the ideal Knapp model as the number of principals identified in 1st order boundary rules increase	Supported Data indicate a more formal relationship among actors and policy process institutions	Inconclusive Expectations are supported – informal process with relevant Top Management identified – yet need comparative case data to reach conclusion	Rejected Formally, the evolution of structure from near Ad Hoc to near formal network occurred when Top Management was named as participants in the Security documents required by PCI.	Supported No formal rules require top management participation; governance structure is deficient in the necessary Knapp processes for areas not under ISMS [367]
H4b: High TMS is likely accompanied by compulsory Boundary rules requiring the participation of a number of principals of the organization.	Supported GT presents compulsory and invitation rules. The number of principles engaged indicates relatively strong TMS and GT presents the Knapp model well	Supported The CIO does employ invitational boundary rules. And, the structure at GS represents the Knapp model well.	Supported Practice currently reveals the structure is deficient in necessary Knapp processes as the participation of top management is declining.	Supported CISO almost a "lone wolf" as she is only one focusing on security policy for an organization among the largest within USG
H4c: If there are no compulsory boundary rules, then the likelihood that a techno-centric governance process increases. TMS will be "lower" than in organizations with compulsory boundary rules.	Supported TMS is indicated within the process institutions	Inconclusive The measure of TMS is the representation of high level management in the policy process. But, there are no compulsory boundary rules found. Yet, indications are that by invitation TMS is achieved.	Supported Directives from the Provost/President created compulsory rules as part of the compliance to USG and PCI demands. But these directives, instigated by PCI audit, are no longer followed – no compulsory rules, weak TMS	Supported GSU has low TMS. The only compulsory boundary rule requires the CIO/CISO as responsible for drafting policy. IT centric – suggesting ad hoc policy structure
H5a: The presence of Open Boundary Rules setting the criteria for participation in making security policy reflects an organizational condition that values collaboration.	Supports Individuals may opt in, criteria for participation on committee also clear.	Supported Requires heavy reliance on rules-in-use. There is an informal open boundary allowing anyone to contribute to specification of needs or feedback to proposals.	Supported No open boundary rules identified, and the structure presents Knapp deficiencies.	Supported No open boundary rules found. Policy structure looks has Knapp deficiencies.
H5b: The absence of an invitation boundary rule specifying participation of university leadership will increase the likelihood of a	Supported GT specifies TMS participation via a number of boundary rules. Structure resembles Knapp.	Supported GS has invitation boundary rules present. Structure resembles Knapp.	Not Supported Invitation boundary rules exist but use of rule in practice is not clear and there are Knapp deficiencies	Supported The only invitation rule is an administrative advisory committee with scope limited to examining the form of policy, not the content and the resemblance

260

Table 8-1 (continued)

Factor	Georgia Tech (GT)	Georgia Southern (GS)	Univ. of Georgia (UGA)	Georgia State (GSU)
governance structure that is largely ad hoc in nature.				to Knapp is weaker than cases with such rules.
H5c: The presence of symmetric Aggregation rules along with Open Boundary rules reflects existence of a collaborative culture and the governance structure is more likely to resemble a completed Knapp model.	Supported – A configuration of information and choice rules support the notion that a collaborative structure is evident in the rules	Weakly Supported AGILE process supports symmetric choices. However, Formal rules lean toward non-symmetric aggregation rules permitting CIO/CISO to make final arbitration.	Supported A symmetric rule is not identified. And, the structure has weaknesses when compared to Knapp.	Supported A symmetric rule was not found. GSU structure is deficient when compared to Knapp.
H5d: The presence of information rules requiring the exchange of information among actors indicates the existence of a collaborative culture and indicates a stronger governance structure when compared to cases without such rules.	Supported GT specifies a number of channels to communicate with stakeholders during each stage of the process	Supported Information rules requiring exchange are found in the informal and formal rules-in-use. .	Supported This case has a lack of information rules and the structure has no retirement, very weak Risk Assessment and Awareness	Supported The process of information exchange is mostly among the administrative leadership, and is informal (interview data). Governance Structure has weak resemblance to Knapp

In order to understand how TMS directly affects outcomes, I propose additional investigations that would explore in detail the processes that require, permit, or otherwise encourage these actors to influence the structure and content of policy. Models of direct participation would look like the Knapp model. The addition of the ACUPA steps added needed precision and detail to this analysis. I would further explore integrating these 'sub-processes' to enrich the analysis. McGinnis and others (O'Toole Jr. 1997; Blomquist and deLeon 2011; McGinnis 2011b; Aligica and Boettke 2009; Cole, Epstein, and McGinnis 2014) have suggested that policy decisions are influenced by processes and actors that are "networked" to the particular policy process of interest. Identification of the linkages between these secondary networks of influence may sharpen the understanding of the structure of an organization's policy governance.

8.2.3.2 Collaboration and Autonomy

The fifth set of hypotheses explored the relationship between structure and the organizational conditions of collaboration and autonomy. Analysis showed a strong presence of Open Boundary Rules (e.g. rules structured to encourage voluntary participation by other actors) in the cases with more formal governance structures. However, "open" seemed to operate as a relative term as we found that the definition of who may be included may be controlled by one or two actors. Terms identified in the Attributes and Conditions of the boundary rules were seen as ambiguous, allowing actors to assume authority to define, or use, the term as they perceived to be proper. The lack of monitoring of the performance of policy processes in all cases prevents both

the case and the USG from understanding the effects that a "narrowing" of participation may bring to policy outcomes.

On the other hand, findings from the GT and GS cases show the positive effects that openness may have on the policy process. Time required to propose, discuss, draft, and approve a policy was found to be significantly shorter for these two cases when compared to UGA and GSU. Some of the "speed" of policy development can be traced to the distributed network structure employed by GT to engage a diverse population of GT representing most if not all of the organizational structure.

The reluctance of both UGA and GSU to pursue policy change due to the amount of time required, up to 24 months, is noted in the respective interviews for the CISO of each case. Both cases are larger, in terms of population, than GT or GS. And, the logistics of managing meetings and feedback is daunting. However, structural features were identified at GSU that further complicate efforts to collaborate. Before a policy at GSU can be discussed among the disparate division, the GSU CISO needs the blessing of both the Office of Legal Affairs and the CIO. With few resources, winning an argument, as to whether a new policy is needed versus maintaining the status quo of an umbrella policy, is in itself a major disincentive to pursuing policy change.

The reluctance at UGA seemed driven by the cost of pursuing policy change versus simply inserting a reference to the requirement into existing policy documents. This reasoning reflects a rational economic decision weighing the time and effort to persuade a disparate community of the need for new policy versus the benefit of that

policy. Given the lack of structure monitoring, the perceived benefit of new policy is likely to be low and the perceived cost of the process very high.

Information rules play an important role in any process that encourages collaboration, feedback, and learning. Information rules play a key role in the identification of structural features that support, and therefore indicate, organizational conditions regarding collaboration. The lack of strength, or presence, of information rules also indicate an organizational condition that values autonomy. The presence, or not, of invitational boundary rules (that encourage participation) along with the presence of information rules further defines the relative strength of a structure that supports, or not, collaboration.

Even though a structure may present the necessary information and boundary rules to support collaborative policy development efforts, the effect of these rules may be constrained by the lack of aggregation rules that determine how a final decision is made. If an aggregation rule is symmetric, supporting a means of achieving consensus, then support for collaboration is stronger than if the rule is non-symmetric. A non-symmetric aggregation rule may allow a CIO, CISO, or Legal Affairs officer, the means of ignoring, or discouraging, a consensus. Further, the frequency of interactions specified by the conditions within information rules may indicate whether collaboration is indeed a value that is strong within the organization or not.

Future research will explore the paired concepts of collaboration and autonomy in greater detail. This study suggests that there are ways to structure rules-in-form to suggest collaboration while defeating the intent of collaboration through various

configurations of rules that value autonomy. A field study involving interviews of many actors across different units of an organization could identify the structure of these arrangements.

8.2.4 Elements of Policy Structure

The units of observation were confined to include those statements that are coded for the Knapp processes of Awareness, Implementation, Monitoring, and Enforcement. Four hypothesis tested the existence and strength of four elements of policy structure (Table 8-2). I discuss those findings below.

Table 8-2 Elements of Policy Structure

Hypothesis	Element Tested	Conclusion
H7: As an organization's governance structure declines from Formal to Ad Hoc, then it is less likely to present a coherent set of standards, procedures, guidelines and policies appropriate for effective policy.	Components	**Not Supported** Count data of component statements not sufficient to explain the structure.
H8: The likelihood of coverage of USG issues will correlate with the relative strength of top management support for securing cyber assets	Scope	**Not Supported** Test of data may not be precise enough to measure realtionship
H9: Acceptable Use Policies will vary in "fit" as the governance structure varies. A Formal structure will provide greater evidence of fit, measured in terms of specific assignments and positions referencing that particular organization.	Fit	**Supported** Precision greatly enhanced with use of institutional analysis tools – grammar and rule configurations
H10: As the governance structure of a university becomes more formal, then the likelihood increases that clarity of the policy is more appropriate to the comprehension skills of the university's student population.	Form	**Not Supported** Results are mixed.

8.2.4.1 Components

The contrast between Georgia State and Georgia Southern when the component criteria are matched is interesting. As noted in the findings, Georgia State has a strong

informal structure. GSU can't be designated formal due to the absence of a formal meta-policy. On the other hand, GS has a formal meta-policy, but is missing the requirement of cross-referencing issues (a requirement of both informal and formal policy structures). One can argue that without the meta-policy GS is similar to UGA and has an Ad Hoc structure. But, the interview data confirms that the GS processes are strongly influenced by the metapolicy. The relatively short-time period required for policy construction lowers the perceived costs and allows GS to move quickly to adapt new external requirements like the copyright feature of the Higher Education Opportunity Act. UGA had not adopted that requirement, except for publishing an external reference in the old copyright policy document.

The weak findings tying the use of policy components to formality of structure may be explained by the lack of education of policy developers as to the purpose of each component. I coded individual observations to the appropriate component category. In a few instances, the case labeled a document, or section of document, as a guideline, procedure, or policy. The inconsistency, or more likely, the consistency of throwing all components together as one document to be applied to managers, technicians, and users alike – contributes to the lack of observable structure. This finding begs the question, if an analyst can't tell the difference between guidelines and policies – can the individuals who are supposed to implement the policy?

8.2.4.2 Scope

The test of the relationship between top management support, acting as a proxy for formal governance structure, and the scope of policy area coverage was weak at

best. I fault the design of the study for not preparing a more robust measure of this relationship. Perhaps a more appropriate test is one that measures the awareness of both top management and users as to the existence and relevance of a policy area solution. Methods such as Q-sort have been used in other studies employing the IAD framework to measure policy compliance and divergence (S. Siddiki et al. 2011; S. Siddiki, Basurto, and Weible 2012; Carter et al. 2013; Feiock et al. 2014; Carter et al. 2015). Additional interviews may also serve to understand the relationship between policy compliance to external requirements and policy scope in response to perceived threats to organizational security.

8.2.4.3 Tailoring (Fit)

The analysis to identify how organizations tailor statements to improve policy fit to the organizational mission and objectives was perhaps the strongest indication of the power of the IAD tools to contribute to analyzing structure. Counts of statements combined with the nested analysis of those statements to aggregate the story of "who does what to whom and under what conditions" created compelling evidence to show that the structure of policy increases in specificity to organizational conditions as the governance structure grows more formal. The demonstration of fit also validates the rudimentary measures of relative strength of Knapp processes that were used to confirm coding of governance and policy structure discussed earlier.

8.2.4.4 Form

Testing the Form of policy as a measure of clarity and understanding is a sensible expectation of whether a policy document and its contents are constructed to be

effectively understood by the individuals whose behaviors are to be regulated. However, the test of readability was flawed. Most of the observations are collected from "one-size-fits-all" documents that included policy statements meant for managers, standards and procedures meant for technicians, and ancillary documents with references for attorneys. As a matter of practice, this form does not bode well for improving the understanding of a student or professor as to the acceptable use of university IT resources. Relating a simple readability test to that understanding belies the complexity of educating individuals as to the expectations of behavior that are heavily dependent upon the role those individuals assume within the organization. I propose future research will need to explore how policies are constructed, published and disseminated in role-appropriate forms as a means of improving policy awareness and effectiveness.

8.3 Discussion Summary

What do we know or understand as a result of this research? How does the structure of cybersecurity policy relate to the structure of policy governance? Does an understanding of governance structure contribute to predicting, or explaining, likely policy outcomes, such as effectiveness? Are the concepts and tools developed for the IAD framework appropriate and effective for discerning these questions? Can we evaluate both governance and policy structure with these tools in a way that contributes to improved security practices?

The evidence shows variation in the actors and the institutions that govern the interactions of those actors among all four cases. In short, structure does matter and the ability of the framework to identify differences in structure is an important contribution to policy design and evaluation (Carter et al. 2013; Carter et al. 2015; Feiock et al. 2014).

The strongest structure is found in the case of Georgia Tech. Members of Top Management are required to oversee a structured, step-by-step process that mandates collaboration among all segments of the university through a series of information and aggregation rules that set "consensus" as a standard to be achieved prior to adopting a new policy. Georgia Tech formalizes policy governance in a document and has "institutionalized" the process by repeatedly employing the process to revise and replace most of the institutions used to govern policy areas such as Acceptable Use, Copyright protection, and Data Protection. Georgia Southern has a similar policy process document but without the formal institutions declaring participation of Top Management and setting consensus as a required outcome. However, Georgia Southern has institutionalized norms and standards similar to the Georgia Tech policy via its implementation of the AGILE philosophy applied to policy making. The commitment of the Georgia Southern CIO to following the AGILE philosophy is a key factor in the success of institutionalizing these values, norms, and standards. The perspective of an individual's interpretation of "rules" is an important aspect of deterrence theory which plays an important part in the construction of cyber security

policy (D'Arcy and Herath 2011). The ability of the IAD tools to identify and compare formal and informal institutions is suggested by Siddiki, et al (2010).

Formality of structure at the remaining two cases is found to be lacking, despite documented attempts to formalize such structure. UGA created a plan that required Top Management Support similar to Georgia Tech's. However, the plan focused on solving the requirements mandated by representatives of the Payment Card Industry as a response to serious credit card data breaches. Other issues, such as copyright protection, data protection, and privacy, have been "solved" by referencing external mandates. This solution requires the least effort to "amend" university policy and achieves compliance on its face. However, the solution also avoids efforts to integrate the policy goals with organizational goals, mission, and culture. Critical processes such as Awareness and Enforcement are not addressed via the process of using references to external mandates.

Georgia State has adopted the ISO 27001 standard for policy governance for 3 departments, leaving the university's remaining operational units and its academic division to abide by an existing "umbrella" policy that has generic standards and goals with a few specific policy areas addressed by documents authored priot to 2005. The work of identifying policy issues and creating a policy revision is done by the university Information Security Office without the collaborative efforts of university top management. A single point of contact, the Office of Legal Affairs, preserves the status quo by insisting that the current umbrella policy is sufficient, unless overwhelming evidence is offered otherwise. Weak top management support is also indicated by the

lack of resources allocated to the Information Security Office which has two employees to manage security efforts for more than 33,000 students and several thousand employees. The implementation of the ISO 27001 standard is limited to the three departments because of the inability of the CISO to get additional funds budgeted to expand the project to other areas of the university.

While not conclusive, hypotheses testing the relationship of governance structure to policy structure in the context of organizational factors such as Top Management Support, Collaboration, and Autonomy, indicates continued support of findings from other research as well as positive indications that institutional analysis can contribute to identifying evidence of how these concepts are "institutionalized", thus becoming part of the formal structure of the organization. These findings are sympathetic to efforts to explain collaboration (Calanni et al. 2014; S. N. Siddiki et al. 2015) or the need for coercion (S. N. Siddiki 2013), and the likelihood of successful policy making exercises.

As to the discussion of the elements of policy structure; components, tailoring, fit, and form are concepts that may not have been fairly investigated within this research design. The elements are largely qualitative in nature, but could be evaluated using quantitative measures given a more appropriate research design. Moreover, the effects of these elements may be better understood in the context of user perspectives. Such perspectives can be identified with surveys, Q-sort analysis, and interviews using the snowball method.

How do the different approaches to policy among the cases contribute to more or less effective cybersecurity? First, remember that effectiveness in this study is measured by identifying processes and practices that practitioners and theoreticians alike agree are necessary to assure effectiveness. The study did not measure the concept of effectiveness directly for two reasons. First, the reluctance of organizations to share their relative exposure to compromises in security is well documented. Second, a casual question to the CISO's of the cases revealed that reluctance is real. Analyzing effectiveness indirectly, by comparing the structure of policy and policy processes, is the only available path given this reluctance.

So, given that effectiveness is measured in this way, do differences in policy governance lead to more or less effective cybersecurity within the universities examined? I believe the answer to the question is affirmative. I offer three reasons why.

First, security literature and popular literature denote the need for dynamic policy governance to respond to ever changing threats and conditions. The two strongest governance structures, Georgia Tech and Georgia Southern, can produce new policy, or policy revisions, in four to six months. Georgia State and UGA managers contend their processes take 18-24 months. The prevalent choice for GSU and UGA Top Management is a preference to avoid policy change. GT and Georgia Southern engage faculty, staff, and top management in time efficient process to produce policy changes that address changing conditions. And, the policy changes are created with a wealth of information rules (see Table 6-9) scattered across the policy processes. GSU has a

substantial number of rules that would be in play, if the Office of Legal Affairs allows the process to proceed past the determination of need for a revision. UGA presented only one information rule.

Second, the importance of consensus cannot be overstated. The two structures, GT and Georgia Southern, that facilitate consensus through participation and information exchange will, by design, create policies and practices that are more likely to align with organizational objectives and culture than the structures presented by UGA and GSU. Remember, UGA opts to reference external policy mandates rather than engage the policy change process. There is little doubt that a significant gap exists between language written by policymakers in Atlanta and Washington and the norms found within those respective institutions.

Third, the importance of top management support is reflected, once again, in the structure of GT and Georgia Southern. Georgia Tech, prior to the formalization of its current metapolicy for managing cybersecurity, deferred to the many autonomous units for implementation of policy suggested by the Information Security Office. The new process, with mandated, first order, participation of top management, became a reality once the President of Georgia Tech communicated clearly that the current model was not securing organizational assets and was creating adverse impressions of Georgia Tech that damaged the university's reputation as a leader in security. Georgia Southern's adoption of AGILE philosophy integrated well with the university culture. The participation of top management assured strong alignment of policy objectives with organizational goals.

On the other hand, UGA lost the participation of top management once the credit card access problems were resolved. The topic of security at GSU remained at a level of management that was two steps below the cabinet. In both cases, only limited changes to security policy occurred in the time frame referenced by this study.

Governance structure determines the likelihood that a policy statement or practice will reflect organizational culture and organizational factors such as top management support. Governance can determine how responsive policy making is to the organization's changing threat environment. My findings in regards to the "fit" hypothesis (#9) support this conclusion, which aligns with findings of other studies discussed in chapters 2 and 3. In retrospect, perhaps the formality of structure (#7), coverage of issues (#8), and form of policy (#10) are related strongly with organizational culture and may actually be a reflection of that culture. Rather than measuring differences in formality of structure, for example, deference should be given to the alignment of governance structure with organizational culture and related factors.

Ostrom's notion of polycentric approaches to find optimum, localized, solutions to common problems supports such a conclusion (E. Ostrom 2010). A polycentric approach challenges suggestions that security ontologies, created to adaptively map security standards to organization's implementations, will best enable inter-organizational comparison, and compliance, of the implementation of security solutions (Ramanauskaite et al. 2013). The notion of an ontology is not the issue, but the creation of a security ontology must be sensitive to the human institutions within which those standards are adopted. For such work, the model adapted for this study may be useful.

In sum, the findings achieved the objectives of this study. The idea of relating features of governance structure to features of policy structure holds promise. How policy is created can determine the structure and effectiveness of policy. The IAD framework and tools are found to contribute towards reliable analysis of the research question and related concepts. I will expand on the implications of this research to the theoretical and pragmatic areas of cybersecurity in the next chapter.

Chapter 9- Conclusion

Breaches, or failures, in cybersecurity is an issue that is considered a strategic threat to our national security and our national economy. Private sector losses due to security breaches have increased and continue to increase. Compromises of payment systems have led to increasingly large losses for retail, finance, healthcare, and even government employers. Postsecondary organizations have not escaped the financial and reputational damage that such breaches create.

Threats to cyber security have many origins and exploit a variety of human, organizational, and technical weaknesses. Knowledge of how organizations structure security policies to meet this myriad of threats within their varying contextual conditions is minimal yet needed (Portnoy and Goodman 2009; Werlinger, Hawkey, and Beznosov 2009). This study focuses on four cases involving research universities to examine the research question: "How does structure of cybersecurity policy relate to differences in structure of policy governance of universities and colleges?"

Why was it important to do this research? The research design is one that addresses this requirement as well as the requirements of the research question. The findings of this study suggest that both the research framework and the tools adapted from other IAD studies are valid, effective means of mapping key features of policy governance and the relationship of the effects of those features upon both the structure of policy and policy management, as well as the potential effectiveness of both within the context of the organization for which the policy is design. The framework provides a

logical guide to future research to tie theory, such as deterrence theory, organizational learning theory, and individual rational choice theory, to policy design and policy practice.

This chapter begins with an examination of the theoretical, policy, and practical implications, of this study. Second, I discuss future directions of research that can expand upon the discussion from the previous chapter. The limitations of the design and findings are discussed. A final thought offers a philosophical perspective as to the value of this and other such works that integrate the human, organizational, and technical perspectives of problems similar to cybersecurity.

9.1 Contributions to Theory, Method, and Practice

One of the objectives of this study is to add to the body of knowledge concerning structure of policy processes (i.e. governance structure) and the outcomes of those processes. The second objective is to demonstrate the utility of analytical tools such as the Institutional Grammar tool and analysis of rules configurations. The third objective was to provide suggestions derived from the study that may aid policy makers and managers in their attempts to create effective cyber security solutions. In the following three sections, I offer arguments as to the attainment of those objectives.

9.1.1 Theory

This study examined the relationship between policy governance and policy through an examination of structure. Precision is enhanced by categorizing observations by policy component, statement type, rule type, and deontic type. The

method to identify and classify governance and information security policy structure builds upon studies by Knapp, Doherty, Baskerville, and others in the following ways.

9.1.1.1 Standard Policy Structure Defined

I expanded the classification of policy structure offered by Doherty, et al (2009). Their study identified structure by policy types and the number of documents that describe standards and procedures. Information security research describes policy structure as a count of documents prescribed for a set of problems. The conceptualization is not a concise, nor precise, means of describing the interaction of actors and institutions assigned to mitigate the problem. For example, analysis of documents for this study identified examples where many policies (defined by area and component) are found in a single document. This study defined structure by terms that include configurations of policy components designed to affect specific policy areas for a given set of actors. This method is not-specific to information security and can be applied, has been applied, to other policy areas (Lubell 2015; Raab, Mannak, and Cambré 2015; Weible and Carter 2015; Feiock et al. 2014).

9.1.1.2 Network of Statements

Statements found in a document may be linked to other policy statements scattered across the legacy of documents for a given organization. This study's framework improves analysis by standardizing the unit of observation on the sentences within each document and then allowing the analysis to place those observations within the appropriate action situation. As theorists from many disciplines have written, it is this network of loosely coupled institutions and actors that actually governs

organizational behavior (Watkins and Westphal 2015; Bryson, Crosby, and Stone 2015; Heikkila 2015; McGinnis and Ostrom 2014; Cole, Epstein, and McGinnis 2014; Weick 1976; Laurence J. O'Toole and Meier 2004).

The disaggregation of the Knapp Action Situations into ACUPA steps offers an opportunity to increase the precision and reliability of analysis of the Knapp model. The ACUPA steps break down the Development box into several action situations connected by their respective outcomes. The aggregation of those outcomes creates policy. Reliability is improved as the ACUPA model is referenced by the USG units. Mapping their instructions into the ACUPA stages allows the analyst to rely on the original text for direction – rather than translating text into the likely categories identified by Knapp (See Table 5-10). Precision of analysis is improved as the analyst can categorize statements into smaller sets of actions containing fewer observations. In addition, the aggregation of observations within categories of activities understood by the managers and policy makers enables validation and application of the results by those who practice what we study.

Future research is needed to validate the incorporation of the sub-processes by surveying practitioners, repeating the original Knapp research design (Knapp et al. 2009). Mapping can identify relationships among stakeholders, the institutions that regulate those relationships and can help managers create coalitions and understanding for policies to be implemented (Aligica 2006). The data from the surveys and the observations from published policies can contribute to the mapping exercise that can identify the interactions of interest.

9.1.1.3 Policy Component

The ordinal ranking of Policy Components created for this study a means to examine observations of institutional statements in categories that describe the roles or particular groups of actors who are responsible for the action or objective of the statement. A component describes the level of action intended. For example, an individual user may be aware of a policy statement that defines an individual's responsibility for securing IT resources but the individual employs a set of procedures to fulfil that responsibility. Management responsibilities for implementing, managing and monitoring policies are found in standards. The rank order of these components is consistent with the instructions and expectations of policies and guidelines published by the Board of Regents, and is consistent with the ontology described within the literature (Neil Francis Doherty, Anastasakis, and Fulford 2009; Baskerville and Siponen 2002; Moule and Giavara 1995). The relative levels of importance correlated nicely with the focus of the research question. However, the study identified some "overlapping" of the categories, particularly at the USG level of policy. These "errors" may contribute to the difficulty of improving policy awareness for all roles across the USG. Confirming and measuring this contribution will be an objective of future research.

9.1.2 Method

Baskerville and Siponen made a cogent argument of the importance of meta-policy to guide emergent organizations in the policy making exercise as they struggle with the challenges of ever-changing context in the form of evolving threats, economic conditions, and organizational challenges (2002). This study was in many ways a

grounded exploration of the application of a meta-theory to explain differences in the outcomes of policy processes among four organizations.

The concept of mapping, and its application, while initially not a focus of the study, developed into perhaps one of the more significant findings. Aligica argues that the IAD framework is a map-making instrument(2006, 75). The IAD framework, in his view, is a meta-theory of institutional mapping. He defines the procedure in three steps: (1) identify and map the action situation and actors; (2) identify factors (environmental and organizational) that affect the action situation; (3) elaborate how the two sets of data found via steps 1 and 2 generate "patterns of interaction and specific outcomes" (p. 89). Those are the steps followed by the design of this study which produced the findings discussed.

Algorithms developed for text analysis can be employed to automate the data gathering from large sets of documents. Analysis similar to that applied in this study can be generated to create the data sets Aligica prescribes. A "big data" project can then look at these patterns over many sets of action situations, with varying degrees of organizational and environmental factors.

9.1.3 Some thoughts regarding application of IGT

This study observed some of the some challenges described by prior research. I offer the following thoughts to further the discussion started by these authors.

9.1.3.1 oBject – Adding to the discussion

The creation of the concept of oBject, the receiver of the aIm, does indeed assist the analyst (Siddiki, et al 2010). I found clarity in resolving the meaning of the Attribute component and in identifying the aIm verb. Classifying what or whom received the prescribed action helps to identify the proper action situation within the ACUPA/Knapp model.

9.1.3.2 Distinguishing between aIms and Conditions

Basurto, et al (2010) called for a better understanding of when the description of the action shifts to qualifiers of the action. I found that limiting the aIm to an action verb as helpful in my analysis. The qualifiers of the aIm are then identified as conditions as suggested by Siddiki, et al (2010). The simpler form of aIm offers a more elegant path to classifying the objectives or goals of the statement and to creating subclasses of the goal by analysis of the conditions that limit the scope of the goal or action.

9.1.3.3 Accounting for implicit effect of Or/Else statements

Studies applying IGT to analysis of institutions note the challenges of implicitly acknowledging sanctions should a norm be violated. For example, Georgia Southern's AUP document has a section that explicitly defines sanctions and how they may be applied should the policy be violated. As the sanctions are part of the document, it is not difficult for the analyst to presume that all norms found in the document are actually rules. I did not resolve this conundrum for this study. But, further application of the tool may be slowed until a resolution is found.

9.1.3.4 Accounting for implicit statements

The difficulty of reliably analyzing statements has been discussed by a number of articles (Basurto et al. 2009; S. Siddiki et al. 2011; Carter et al. 2013). There is a need for consensus regarding the idea of using observations of implicit statements found within formal institutional statements. Research tends to take the conservative approach to using only what is written. However, there are times when the position, boundary, and scope statements are implicit and can be attributed to formal statements. I believe one can validate these implicit statements by seeking the concurrence of actors that these statements are practiced. For example:

336:3 *Policy issues can be identified by anyone within the University community context.*

Using the basic AIM verb of the statement, "Identify", this is a Choice statement. However, the statement implicitly creates the position of "issue identifier" assigned to the attribute "anyone within the University community context". The attribute - "anyone within the University community context" – sets the boundary for who is eligible to hold the position of identifier. Finally, the statement specifies that a single individual may identify a need – and can be classified as an Aggregation statement. The implicit statements "fill in the blanks" by describing the structure of the action situation focused on issue identification.

9.1.3.5 Accounting for statements present across multiple action situations

I found a number of observations that can be coded for multiple action situations. For example, within the Information Security Management System (Doc 367), GSU has a rule that says:

> *When a new procedure, or version of a procedure, is issued for inclusion in the University's Information Security Management System it will include:… (Ref 367:13)*

The Condition "when a new procedure" applies to the Knapp Development situation. The Condition "or version of a procedure" implies a revision of existing policy and applies to the Knapp Review situation. One can code the same observation as a member of those two sets. Or, one can create two separate observations, one for each relevant situation. Clearly, a standard is required to assure the reliability of the "count" of observations included in the structure of each situation.

9.1.4 Policy and Practice

Those working in the information security discipline (Baskerville and Mikko Siponen 2002; Dhillon and Backhouse 2001; Kolkowska and Dhillon 2013; M. Siponen, Pahnila, and Mahmood 2010;), as well as the public policy discipline (Hicklin and Godwin 2009; O'Toole Jr. 2000; L. J. O'Toole 2004; Robichau and Lynn Jr. 2009; Simon 1973) have opined as to the need for research to be relevant to practitioners. I offer four suggestions that, while not exhaustive, do demonstrate contributions to meeting that need.

First, the research model provides some insight as to components critical to consensus building within university governance structures that have been labeled as

"organized anarchies" or garbage cans (Cohen, March, and Olsen 1972). I believe the model is, in reality, a dynamic example of polycentrism. Within the limited domain of a university, approaches to managing access and availability of critical resources such as information technology are not too dissimilar to the efforts of fisherman or foresters who seek to maintain the sustainability of the enterprises through cooperation and information exchange. The two strong examples of Georgia Tech and Georgia Southern demonstrate how a consensus driven approach that emphasizes access to relevant information can be successful in changing organizational culture towards solutions for cybersecurity. The dynamics of security require a flexible approach that is welcomed by the entire organization rather than an approach emphasizing security as a "technical issue" that must be implemented via the authority possessed by those in "positions" of authority.

Second, the IAD framework reminds the managers of the multi-level nature of the security policy process. The interaction of governing organizations at the constitutional level with the policy organization of the university must be accommodated if external conditions to success are to be assured. And, the relationship between the policy as written and the policy as implemented must be acknowledged. The inclusion of actors from the operational level of policy, where the policy is implemented, within the process of creating policy statements and management practices may improve the flow of information that assures operational level knowledge of payoffs, for good and bad behavior, incentives for top management expectations of operational level outcomes, and an appreciation of the importance of

information flow to assure better policy decisions. In sum, the framework points out the necessity of a "feedback loop", long ago acknowledged within the policy stages heuristic, and the cybernetic learning models advanced in the 1940's (Wiener 1948). Such feedback is presented within the ACUPA steps integrated into the research framework and thus provides a structure to assist managers modifying or implementing governance to secure their information technology assets.

Third, the grammar tool, and analysis that follows, offers some applications practical to the managers that draft and implement security policy. Chief among these applications is sensitivity to keeping the structure of the institutions developed to create the policy structure simple. For example, observation [332:15] is a statement found in the AUP policy of Georgia Southern. I originally coded as an Aggregation rule type upon my judgement that "responsible" gives the user control for the action taken in terms of using that resource.

> **Each user of a university IT resource [A] is [D] responsible [I] resource [B] ultimately for the use of that resource [C]**

The phrase "is responsible" can be argued is equivalent to "shall be" – (is – a form of the phrase 'to be') – making this a position verb by definition. The statement could be re-written as:

> **Each use of a university IT resource [A] shall [D] be [I] responsible for the use of that resource**

Or could be written as;

> **Each user of a university IT resources shall [D] use [I] that resource [B] responsibly [C]**

This sentence is a Choice statement – “responsibly” is a Condition as it describes “how” the user will use the resource. Given the level of analysis is “Operational”- reducing the statement to a straightforward institution of Rule Type Choice provides the user with clear instructions.

Another example of improving the comprehension of statements by the intended actors is the statement [332:18]:

> *In the event that misuse of IT resources threatens to compromise the integrity or jeopardize the security of university resources or harm authorized users of those resources, the University's Chief Information Officer, or his or her designee, is authorized to take any and all necessary actions, including the immediate confiscation and/or disabling of a university resource or the temporary or permanent termination of user access credentials, to protect, investigate, and ensure the security and proper use of IT resources.*

The statement is constructed of 80 words and scores a Flesch-Kincaid Reading level of 39 (as in years of education). The statement is grammatically challenged, and presents the reader with confusion as to what verb applies to which phrase and condition. Coding the statement using IGT, the statement decomposes to:

Table 9-1 Example Decomposed Statement

Attribute	University's Chief Information Officer, or his or her designee,
Deontic	Is
Aim	Authorized
Condition	to protect, investigate, and ensure the security and proper use of IT resources; In the event that misuse of IT resources threatens to compromise the integrity or jeopardize the security of university resources or harm authorized users of those resources,
Or Else	
Object	any and all necessary actions, including the immediate confiscation and/or disabling of a university resource or the temporary or permanent termination of user access credentials

Rather than speak in terms of “authority” [if authority is the AIM, then the attribute must be the university president who authorizes the CIO (object) to take actions

(Conditions) – which does not make the user the object of the policy] – we reduce the statement to:

Table 9-2 Example Reduced Statement

Attribute	University's Chief Information Officer, or his or her designee,
Deontic	May
Aim	Take
Condition	to protect, investigate, and ensure the security and proper use of IT resources; In the event that misuse of IT resources threatens to compromise the integrity or jeopardize the security of university resources or harm authorized users of those resources,
Or Else	
Object	any and all necessary actions, including the immediate confiscation and/or disabling of a university resource or the temporary or permanent termination of user access credentials

Further simplification leads to:

> *The University's Chief Information Office, or his or her designee, may take any and all necessary actions to protect --- etc.*

In general, refined rules for following the grammar and the ideal structure of a policy action situation may lead to policy structures that are less ambiguous to read and the outcomes of which are more clearly understood by the participants.

Finally, the model presents a structured approach to link contributions of theory to the structure of policy governance and policy. For example. deterrence theory forms the foundation of much research that emphasizes the awareness of "penalties" of individuals who choose not to follow policy statements. Clearly, without well-structured awareness activities, reliable compliance procedures and enforcement procedures that produce outcomes consistent with the "or else" component of the policy, the expected outcomes predicted by deterrence theory will not be observed. The model provides the type of map that will aid managers as they try to understand why a policy process is

frustrated by organizational norms, and how those norms may be adapted to assure future success. Of course, future research can help by providing models and simulation tools that help the manager anticipate challenges in the governance of policy, as well as the operationalization of policy.

9.2 Future Research

A research design for analysis of "the design of city charters" used many of the methods found in my study of university policy governance (Feiock et al. 2014). The objective of the Feiock study was to identify certain configurations of institutions aligned with types of charter structure. The research agenda prescribed by the authors is one which the authors argue "could generate a more precise and rigorous understanding of the relationship between the difference configurations of institutions of city charters and the politics, governance, and performance of municipalities" (p. 1). Among the agenda items are topics including: examining differences across different forms of government; linking configurations of institutions to government performance; examination of structures as they evolve over time; and analysis of participation of citizens across different structures.

Perhaps the most compelling feature of the research model employed in this study is the capability of the model to support research at many different levels of analysis, yet provide a path so that one may aggregate findings across topics and organizations as well as aggregate "up" findings generated by drilling down through the

many levels of analysis. The feature was demonstrated in this study via the application of the ACUPA model within the Knapp model, as I discussed earlier.

Such an approach can be employed to explore alternative decision models. For example, one could design a research project that would analyze how decisions regarding the content and scope of cybersecurity policy are constrained by the network of policy influencing units and rules within a particular organization. At a department (operational) level, why would any department feel compelled to comply with enforcing acceptable use policies when the university budget office will not supply funds to support such an activity? Why would such a policy be created given the same payoff rule (no resources for implementation) is known? Why would the university president accept such a policy? Why would the governing body (i.e. university board or system board) create a compliance rule that will not be enforced? And, how does the knowledge that such "paper tigers" are the norm, affect the individual's decision to comply, or not, given the risk of enforcement is almost zero?

To take another extreme, at what point are rules so numerous that at both the operational and collective levels, those rules simply "overwhelm" the managers and individuals making payoff rules ineffective? Or, is there a level of information flow that can be identified as a "tipping point" where the linkages between decisions and outcomes are impossible to discern? And, if those linkages are not known, or cannot be measured, is there any structural change that can be made to the policymaking apparatus to create effective policy?

9.2.1 Structure of Workflow and Support

The institutional grammar tool has been applied to test whether individuals perceive policy designs as appropriate or too coercive (S. N. Siddiki 2013). The effects of rules must be considered in context of all other rules and norms that structure organizational behavior (Werlinger et al. 2009; Hawkey et al. 2008; O'Toole and Meier 2015). Essentially, new rules must compete with old rules for the scarce resources of each individual, or team of individuals, that the rule is targeted to affect. Competition creates opportunities for choices to be made by the individual, or team, as to which rule/outcome is important to their success. In sum, a decision is made weighing the benefits of compliance with one rule while accepting possible costs of not complying with others. How do organizational structures affect the operational level decisions to make these choices? How much influence may education programs have on these choices? Is it possible to identify the point of "overload" (i.e. too many policies and too few resources) as a function of policy structure at the operational level? I am particularly interested in how we might model these situations, then test the key model parameters with field research.

9.2.2 Well Structured Policy Systems

The idea that a well-structured policy system has an appropriate mix of components supports concepts important to polycentric governance, an idea espoused by Ostrom as an effective means of local response to global issues (Andersson and Ostrom 2008; Kiser and Ostrom 2000; E. Ostrom 2008b; V. Ostrom, Tiebout, and Warren

1961). One can expect and accept institutional diversity at the level of procedures and guidelines so long as the policy objectives are maintained. Are there institutional configurations within those components that perform better than others? Are those configurations a product of identifiable configurations of organizational factors, environmental factors, or a combination of both? Are there key indicators, "marker genes", that suggest an increased likelihood that policy-making will be more or less effective than similarly situated organizations?

Part of my research agenda is to continue to explore the structure of policy-making procedures across a number of universities, analyzing the structural differences in the context of organizational factors but expand to include efforts to map the structure of processes that create outcomes including budget decisions, departmental planning, and personnel management. Do job descriptions, personnel hiring decisions, and inter-personal relations (i.e. social networks) provide more detail on the position and aggregation rules that may lead to a better understanding of the dynamics of decisions made at both the collective and operational levels? In short, if the hiring manager hires a CIO or CISO with strong technical skills, but weak organizational and people skills, should we expect the new hire to guide a policy process that produces a well-balanced policy structure that can incent both individuals and organizational units to achieve the desired policy outcomes? Can you correct such a feature with different hiring rules, training (awareness), or a well-structured process to improve organizational learning?

9.2.3 Mapping Key Features

Of the many limitations that accompany this study, the focus on a discrete set of institutions representing external and organizational conditions perhaps constrains the application of findings the most. If we are to understand how to design institutions that are tailored to fit each organization's institutional, social, and ecological context then we must understand "how various institutions (and sets of institutions) affecting resources interact with each other"(Cole, Epstein, and McGinnis 2014). In other words, as Cole, et al., surmise: fit is "how rules fit with other rules". Aligica suggests that the most strategic important contribution of the IAD analysis may be mapping such concepts as features within the structure of governance and policy (Aligica 2006).

I discussed how a number of external standards published by the federal government (FISMA and NIST 800), ACUPA (policy governance), ISO 27002, PCI, etc., are offered as guidelines to help USG units construct their individual information security plans. Applying a structured analysis using the framework for this study can aid managers and policy analysts by helping them to a) map the requirements with actors and outcomes; b) understand how internal and external conditions may require tailoring of those standards in order to optimize effectiveness; and c) structure their analysis of post development and implementation of those policies so that the data informs longitudinal studies. Such an analysis helps that organization monitor progress towards security objectives, and cross-sectional studies, by facilitating the analysis of similar and disparate efforts across organizations solving like problems. Understanding the interaction of various sets of constitutional and collective level rule configurations may

inform practitioners and scholars alike of ways to improve the policy process measured by improved likelihood of attaining the desired goals. Mapping the situations may also help managers predict and mitigate potential "negative" interactions among organizational actors.

9.2.4 Social Network Analysis

Collaborative governance and policy networks refer to similar phenomena (Ansell and Gash 2008; Giest and Howlett 2014; Agrawal 2014). We may be observing a shift away from organizations and to networks (Raab, Mannak, and Cambré 2015). Much work has been done on the subject of policy networks, structure and effectiveness (Provan and Kenis 2008). And, the IAD framework has been suggested as an elegant means of advancing research to "more discussion of the relationships of administrative systems to structures and processes beyond rules" (Robichau and Lynn Jr. 2009). Social Network Analysis has been advocated as a means of advancing the study of such phenomena (Sandstrom and Carlsson 2008).

One can approach the topic by mapping the positions described by Attributes to the positions found in the statement Object. Grouping of statements by the aIm (goal) may reveal priorities of concern. Analysis of information rules use concepts such as channels of flow, frequency, and accuracy may add to the discussion (E. Ostrom and Crawford 2005b). Relating these flows as "connectors', thereby establishing the relationships between processes/decisions and the strength of information flow, is analogous to the concept of centrality used in social network analysis. Perhaps one can

applying concepts from social network analysis to understand the "structure" of policy processes and the relationship to policy outcomes. The overlap of these approaches contain much in common that deserves further thought.

9.2.5 Towards "Big Data" Research

A common criticism of the analysis generated by use of the IAD framework and grammar tools is that such work consumes significant human resources. I believe that tools and methods used to mine text offer an opportunity to analyze documents and interview transcripts that will provide an enormous wealth of data that represents organizations across and within sectors such as higher education. Text mining software is available for packages such as R, used in this study, SPSSX, and database packages like MySQL. Moreover, IAD research published within the last 2 years indicates an evolution of the algorithms employed to identify statement types and categories and to further dissect policy statements into the grammatical components. As the reliability and validity of these algorithms are substantiated, these procedures can be coded and shared to expand both the quantity and scope of data available. Simple comparisons of grammatical structure, statement form (i.e. readability), and choice of words used to define attributes, conditions, and objects can be made within an organization by comparing these concepts found in policy documents from significant university or organizational divisions (i.e. academic affairs, technology, business affairs, etc.). And, comparisons can be made across organizations. Initially, findings of a "big data" project may suggest key factors that field research could explore in greater detail.

I think of this opportunity to be the equivalent of building an “atom-smasher”. Theory should predict the types of structure that erupt when policy documents are “busted” into the many statements and grammatical components that compose those documents. Field research can validate and verify the findings. Data technology can improve the reliability of coding, the scale of data sources, and the sharing of knowledge gained.

9.3 Limitations

Ability to draw inferences from this study is constrained by the small sample and the focus on research universities. Such limitations are the nature of a dissertation and, more practically, of the resource limits for most studies of this type. The case study method provided confirmation of prior research as to the direction of effects of concepts like Top Management Support, autonomy, and collaboration. The tools employed did demonstrate utility in understanding diversity of institutions and how those institutions are configured to reflect the external and organizational conditions that constrain policy making and policy implementation in these cases.

One intended outcome of the study was to create sets of rule configurations that correlated with individual organizational conditions. I was unable to create that outcome. The potential of the framework and tools is apparent, however, to create a field of data supportive of mapping such configurations. A larger set of cases is required in order for that to be so. Calls for larger and more diverse data sets are found from similar applications of IAD analytical tools (Feiock et al. 2014; Carter et al. 2015).

Implicit assumptions about rules were most important in understanding the processes. Ostrom and Crawford found that implicit assumptions "might have been the most important drivers of results in earlier analyses of institutional arrangements" (Ostrom and Crawford 2005, 206). However, such assumptions are prone to the bias of the researcher. Replication of the results of this study is needed to affirm or deny the effects of such bias.

The study is also limited by the nature of interpreting linguistic statements representing institutions (Crawford and Ostrom 1995). Whether written or spoken, these statements represent the biases and understandings of those that speak and write them. The interpretation of those statements by individuals whose behavior is to be affected is a significant research challenge long noted in the application of institutional and systems analysis to policy problems. The same limitations apply here

Challenges and limitations derived from my ability to comprehend and accurately apply the IAD framework and its tools are plentiful. Maintaining focus on both the appropriate units of analysis and the correct level of analysis is a terrific challenge in institutional research. Policy documents reflect statements that operate at all three levels of analysis – constitutional, collective, and operational. Discernment of the appropriate level needs a test of reliability.

The focus of this research was at the collective level – separating operational level rules (which are outcomes of collective level decisions) is not easy. All of these levels are "nested" within the larger systems of which the primary organizational unit is a component thus adding difficult to the task of data collection and analysis. If the unit

of analysis is the institutions governing policy, those institutions are regulated by other institutions created in separate areas of the organization. This web of interlinked institutions and action situations operationalize both the culture and the governance structure, at nested levels, that affect the creation of norms and rules.

The validity and reliability of coding statements as policy components (Meta policy, policy, standards, etc.) needs further investigation. A simple test employing multiple coders would certainly suggest problems regarding reliability. The validity of the concept needs further examination as well. The difference between a meta-policy, policy, and standard can be made with the choice of a word or two.

Of course, some of the errors of the study attributed to my individual biases and weaknesses can, of course, be mitigated via replication and the use of multiple coders in future studies.

9.4 Conclusions

The topic of this study is one that has origins from my time spent as the assistant to the CIO for the University System of Georgia. I observed a tremendous effort by the Board of Regents, system staff, and more than 60 college and university CIO's and CISO's, to create policy to secure tens of thousands of networked devices, terabytes of data, and millions of dollars in large computing and networking resources. Despite the strong collaborative efforts, a diverse universe of policy documents were found among the then 35 organizations governed by the Board of Regents.

My simple question of "why" such a diversity of security policies existed led directly to the effort documented by this exercise. The importance of understanding "why" is one that is explained by decades of security research, both academic and practical, and is indirectly supported by the investment of public and private funds into organizations such as the Cybersecurity Division of the Department of Homeland Security, The United States Cyber Command within the U.S. Department of Defense, the International Standards Organization (ISO), and the Payment Card Industry (PCI), to name a few. Numerous studies continue to call for an understanding as to how policy goals may be achieved while preserving autonomy and integrity of the organizations the policies are designed to protect.

While the limitations of this study are substantial, the promise of the approach is one that is confirmed by the findings discussed in chapter 8, several related research publications that are referenced, and the suggestions for future research provided in this chapter. The research framework and tools employed suggest that a reliable and valid means of coordinating such future research can address the high-level need to contextualize policy solutions to local factors while preserving the intended goals and outcomes of policy design. The potential of the method to create "big data" suggests that models can be suggested for a range of organizational factors, thus providing guidance to practitioners of policy so those practitioners may achieve measured progress towards their security goals.

The problem of securing cyber space is one that cannot be isolated from the human, organizational and technical challenges that are commonly found in

organizations attempting to secure information resources from harm. Studies involving institutions and the governance of shared resources often reference Garrett Hardin's "Tragedy of the Commons". The idea of how to prevent the "over grazing" of a public commons is often described as a simple, straight-forward discussion of how private behaviors may best be incented to avoid an outcome that negatively affects everyone. A re-examination of the premise of the 1968 article claims that prior approaches to the commons problem are grossly over-simplified (Cole, Epstein, and McGinnis 2014). The concluding paragraph of this award-winning article[47] also sums up the strategy expressed by many information security researchers and analysts that must be considered as we are strive to secure our information assets.

> The open-access pasture does not exist in splendid isolation but operates within a larger universe of interacting resources and institutions. Hardin's 'tragedy of the commons' is not just about the pasture; it is equally about the grass, the cows, the herders, and the human society. (Cole, Epstein, and McGinnis 2014)

[47] The article won the 2015 Elinor Ostrom Prize for the best full-length article published during the previous year in the Journal of Institutional Economics.

Appendix A Summary Case Data

Case	Initials	Compliant	Student Pop Spr 12	Carnegie Basic	Carnegie Basic
Abraham Baldwin Agricultural College	ABAC	4	3002	AA	Assoc/Pub4
Gainesville State College	GSC	6	7919	AA	Assoc/Pub4
Gordon College	Gordon	5	4245	AA	Assoc/Pub4
Middle Georgia College	MGC	2	2985	AA	Assoc/Pub4
Georgia Perimeter College	GPC	9	25616	AA	Assoc/Pub-M-Sc
Bainbridge College	Bainbridge	3	3681	AA	Assoc/Pub-R-M
College of Coastal Georgia	CCGA	2	3063	AA	Assoc/Pub-R-M
Darton College	Darton	3	5899	AA	Assoc/Pub-R-M
Georgia Highlands College	GHC	8	5462	AA	Assoc/Pub-R-M
East Georgia College	EGA	5	3130	AA	Assoc/Pub-R-S
South Georgia College	SGC	1	2090	AA	Assoc/Pub-R-S
Waycross College	Waycross	6	993	AA	Assoc/Pub-R-S
Atlanta Metropolitan	ATLM		2765	AA	Assoc/Pub-U-SC
Savannah State University	SSU	12	4134	BA	BAC/A&S
Dalton State College	DSC	7	4978	BA	Bac/Assoc
Clayton State University	Clayton	4	6872	BA	Bac/Diverse
Fort Valley State University	FVSU	5	3674	BA	Bac/Diverse
Georgia Gwinnett College	GGC		8047	BA	Bac/Diverse
Macon State College	MSC	5	5569	BA	Bac/Diverse
Armstrong Atlantic State University	AASU	4	7013	MA	Masters L
Augusta State University	AUG	3	6381	MA	Masters L
Columbus State University	CSU	6	7803	MA	Masters L
Georgia College & State University	GCSU	10	6266	MA	Masters L
Kennesaw State University	KSU	8	23103	MA	Masters L
North Georgia College and State University	NGCSU	8	5934	MA	Masters L
University of West Georgia	UWG	5	10933	MA	Masters L
Valdosta State University	VSU	3	12277	MA	Masters L
Albany State University	ASURAMS	6	4360	MA	Masters M
Southern Polytechnic State University	SPSU	3	5530	MA	Masters M
Georgia Southwestern State University	GSW	3	2916	MA	Masters S
Georgia Southern University	GaSou	7	19150	RU	RU/D
Georgia Institute of Technology	GT	8	19431	RU	RU/VH
Georgia State University	GSU	8	30606	RU	RU/VH
University of Georgia	UGA	8	33367	RU	RU/VH
Georgia Health Sciences University (GRU)	GHSU	8	2780	RU	Spec/Med

Appendix B Policy Inventory

Case		# USG Required Policies	USG Info Sec Policy Section 11 (2011)	USG Password Authentication Policy	USG Appropriate Use Policy	USG Risk Management Policy	USG Data Handling and Storage Standard	USG Computer Security Incident Management Policy	Web Privacy Policy	USG - HIPAA Privacy and Security Policy	USG Continuity of Operations Plan	Use of Cryptography	Security and Awareness Program	Electronic Data Disposal	Copyright Violation Guideline (405)
Abraham Baldwin Agricultural College	ABAC	4	✓		✓		✓						✓		
Gainesville State College	GSC	6	✓	✓	✓		✓							✓	✓
Gordon College	Gordon	5	✓		✓		✓		✓						✓
Middle Georgia College	MGC	2			✓					✓					
Georgia Perimeter College	GPC	9	✓	✓	✓		✓	✓	✓		✓	✓	✓		
Bainbridge College	Bainbridge	3			✓				✓						✓
College of Coastal Georgia	CCGA	2	✓		✓										
Darton College	Darton	3	✓		✓		✓								
Georgia Highlands College	GHC	8	✓	✓	✓	✓	✓	✓	✓			✓			
East Georgia College	EGA	5			✓		✓	✓	✓						

Appendix B Policy Inventory

Case		# USG Required Policies	USG Info Sec Policy Section 11 (2011)	USG Password Authentication Policy	USG Appropriate Use Policy	USG Risk Management Policy	USG Data Handling and Storage Standard	USG Computer Security Incident Management Policy	Web Privacy Policy	USG - HIPAA Privacy and Security Policy	USG Continuity of Operations Plan	Use of Cryptography	Security and Awareness Program	Electronic Data Disposal	Copyright Violation Guideline (405)
South Georgia College	SGC	1			✓										
Waycross College	Waycross	6	✓	✓	✓		✓	✓						✓	
Atlanta Metropolitan	ATLM														
Savannah State University	SSU	12	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓
Dalton State College	DSC	7	✓	✓	✓		✓	✓			✓				✓
Clayton State University	Clayton	4	✓		✓									✓	✓
Fort Valley State University	FVSU	5													
Georgia Gwinnett College	GGC														
Macon State College	MSC	5		✓	✓		✓	✓							✓
Armstrong Atlantic State University	AASU	4	✓	✓	✓		✓								

Appendix B Policy Inventory

Case		# USG Required Policies	USG Info Sec Policy Section 11 (2011)	USG Password Authentication Policy	USG Appropriate Use Policy	USG Risk Management Policy	USG Data Handling and Storage Standard	USG Computer Security Incident Management Policy	Web Privacy Policy	USG - HIPAA Privacy and Security Policy	USG Continuity of Operations Plan	Use of Cryptography	Security and Awareness Program	Electronic Data Disposal	Copyright Violation Guideline (405)
Augusta State Universiity	AUG	3	✓		✓		✓								
Columbus State University	CSU	6	✓	✓	✓		✓		✓		✓				
Georgia College & State University	GCSU	10	✓	✓	✓		✓	✓	✓			✓	✓	✓	✓
Kennesaw State University	KSU	8	✓	✓	✓	✓	✓	✓	✓					✓	
North Georgia College and State University	NGCSU	8	✓	✓	✓	✓	✓	✓						✓	✓
University of West Georgia	UWG	5	✓	✓	✓				✓						✓
Valdosta State University	VSU	3	✓		✓	✓									
Albany State University	ASURAMS	6	✓	✓	✓	✓	✓							✓	

Appendix B Policy Inventory

Case		# USG Required Policies	USG Info Sec Policy Section 11 (2011)	USG Password Authentication Policy	USG Appropriate Use Policy	USG Risk Management Policy	USG Data Handling and Storage Standard	USG Computer Security Incident Management Policy	Web Privacy Policy	USG - HIPAA Privacy and Security Policy	USG Continuity of Operations Plan	Use of Cryptography	Security and Awareness Program	Electronic Data Disposal	Copyright Violation Guideline (405)
Southern Polytechnic State University	SPSU	3		✓	✓										✓
Georgia Southwestern State University	GSW	3	✓		✓				✓						
Georgia Southern University	GaSou	7	✓	✓	✓		✓	✓		✓					✓
Georgia Institute of Technology	GT	8	✓	✓	✓	✓	✓	✓	✓						✓
Georgia State University	GSU	8	✓	✓	✓	✓	✓	✓	✓	✓					
University of Georgia	UGA	8	✓	✓	✓	✓	✓		✓					✓	✓
Georgia Health Sciences University	GHSU	8	✓	✓	✓	✓	✓			✓	✓			✓	

Appendix C Document Protocol

1. Policy Inventory
    a. Every policy document found on a USG unit site receives a unique id number, serialized, to serve as a reference throughout the database
    b. The following data is contained in the table called 'Document'

Table C-1 Document Data Table Layout

Variable Name	Description
DocID	Primary key – id number unique to each policy document
DocName	The title of the policy document, will most likely reflect the policy issue addressed by the document
Policy Scope	Details which type of policy per the Table 4-4 Taxonomy
Event/Contact	Where the document was located – usually from the website of the case
Significance	Why the document is important
Summary	Summarizes purpose of the document
Organization	The unit which owns the document
Case_id	The key for the organization as inventoried in the case protocol
e-location	The url where the document was located when catalogued
Date received	When the document was catalogued
Date Effective	When policy took effect
Date Revised	Notes latest revision of document
Date_last_accessed	When last seen on web
Misc	Place for analyst notes
Policy Administration	Who/What department responsible for creation, management, maintenance of document

2. Code Document Meta Data

Table C-2 Meta Data Variables

Step	Variable	Action
1	Acquire Document	Acquire the document -- If the document is not in a pdf, convert to one so that Adobe edit tools can be used to ascribe notes to the document for later review. Name the pdf with the following bits of information Unit Name Policy Doc Name (e.g. Acceptable Use, Malware, etc) Blank if original – "Analysis" if this is copy with notes from researchers
2	Doc Name; Policy Title	Take the Document name explicitly given the document – if none provided, name and reflect how the name was conceived. Other variable reference – Policy Title
3	Date Received Date Effective Date Revised	Dates: Date Received – indicate the date you accessed policy via web, or received otherwise (mail, etc) Date Effective, Date_Revise – take dates as found in policy document. If blank, then no dates were found.
	Date Last Accessed	Most recent date that researcher accessed the file
	Responsible Official	Name of official responsible for administering the policy – as found in the document
	Authorized by	Entity responsible for formalizing, placing policy within university functions
	Policy Administration	Who or what department is responsible for creation, management, maintenance of the document -i.e. primary office responsible
4	e-location	Identify Policy URL
5	USG Unit, Unit ID	Identify USG Unit and Unit ID
6	Objectives	Take from stated purpose of policy -- the stated aims of the policy. These were found by the Doherty study in the introductory statements. A clear reference to objectives is considered a best practice.
	Summary	
	Policy Class	Categories: Policy, Standard, Guideline – definitions found (seek reference)
7	Policy Scope	Doherty names this "Policy Coverage" – records policy areas covered… While objectives indicate scope (Doherty 2011), the coverage of issues identified by best practice studies will be used to measure scope. Each policy document is reviewed to identify the explicit policy issues or areas covered. References to external policies are not considered in this analysis. A pattern of missing areas will document "defective" policy
8	Policy Focus	Individual – focuses on behavior management

Table C-2 Meta Data Variables (continued)

		Process – focuses on procedures, organizational behavior Technology – focuses on management of technical issues such as bots, filtering, etc.
9	Policy References	List all external policies, laws, regulations referenced explicitly in the document
10	Policy Administration	Id individuals responsible for managing policy and references to procedures to update policy
11	Policy Structure	Doherty observed the following variables: Which types of policy are available? How many policies compose the policy? How do they relate to each other? How do they relate to lower level standards and procedures?
12	Form – Flesch Kincaid Score	Calculated by Microsoft Word Review function –score indicates the grade level for reading skills necessary to comprehend the document
13	Form – Flesh Reading Ease	Calculated by Microsoft Word Review function – score indicates the readability of the document. Long words affect this score significantly more than they do the grade level score. See Wikipedia entry (http://en.wikipedia.org/wiki/Flesch%E2%80%93Kincaid_readability_test#Flesch_Reading_Ease) for excellent summary
	Length	Number of words in document – calculated by MS Word Review
	Length-statements	Number of sentences – calculated by MS Word Review
	USG Policy Link	Meeting critieria of this USG policy(s)

Comments:

Documents are linked to cases (e.g USG Unit)

1. Policy Objectives – the stated aims of the policy. These were found by the Doherty study in the introductory statements. A clear reference to objectives is considered a best practice. Objectives must be clearly stated within the document (2011. 203).
2. Policy Scope – Doherty names this “Policy Coverage” – records policy areas covered… While objectives indicate scope (Doherty 2011), the specific policy areas, are identified by studying the content of the policy and comparing to the isses that best practice studies indicate should be present (2011, 204). Each policy document is reviewed to identify the explicit policy issues or areas

covered. References to external policies are not considered in this analysis. A pattern of missing areas will document "defective" policy.

Determination of coverage will occur after the IGT tool has parsed the individual units of observation. The units of observation, or individual policy statements, will be assessed using the Taxonomy of Security issues developed by Doherty, et al.

3. Policy Structure – Doherty relies on the title of the policy – he is building a portfolio – and calling that structure – with some support from the literature. – the crosstab works for this exercise.
    A) Which types of policy are available;
    Method
        a. Capture policy title
        b. Review objective for the policy – identify Policy type based upon the Doherty Table 4-3
        c. Code for each type the policy explicitly mentions

    B) How many policies compose the entire policy?
        a. A count of the policy documents related to the types of the security policies
    C) Policy References – details of links to internal ancillary policies, external policies, legal mandates, etc – A xtab of policy document vs policy references could be demonstrative here…

Appendix D Data Dictionary – Case Summary Data

Variable	Description
Case ID	Identifying number
Case	Official Name of Campus
Case_initials	Abbreviation
Mission	Carnegie Class of AA (Associate Degrees), BA (Bachelors), MA (Masters and some limited doctoral degrees, RU – (Research University)
Student Pop	Enrollment as of 2012
URL	Web page locator for main campus page
Case_Cysec	Primary URL for Page with links to cyber security policy
Case_Contact	Individual that served as main liaison between the campus and investigator
Case_Phone	**Identity of person used as key contact for the unit**
ISO Reference	**URL page link for Information Security Office page (if available)**
Policies Reference	**URL page link for cyber security policies page**
Contact Email	**Email address**
Security Officer	**Individual accountable for enforcing cyber security**
Security Officer title	
Carnegie_Classification_ID	**Link to Carnegie reference information**
USG_Classification_ID	**Link to USG Classification**
Security Phone	**ISO phone number**

Appendix E Document Summary – Meta-Data

Policy Document Data Summary

Organization:	Office of Governor	Case_id:	42
DocName:	Gov Exec Order	DocId:	6
e-location:	http://gov.georgia.gov/vgn/images/portal/cit_1210/32/5/109335759 03_19_08_01.pdf	Policy Classification	Guideline
Policy Type	Information Security, Governance	Policy Area	Awareness and Training BS 17999 reference Compliance with legislation Contingency / continuity plan or 27000 HPEOA It is essential that all
# Words:		# statements	
Flesch-Kincaid:		Flesch Reading Ease	
Date Recd:	5/1/2010	Date_issued:	3/19/2008
Authorized by:		Date_Effective:	
Date_Rev:		Responsible Office	CIO
Responsible Official:		Responsible Official email:	
Policy Objective	The Executive Order calls for a single set of information security reporting standards for all agencies to follow. Currently, state agencies use a variety of reporting standards, making it difficult to measure information security across state government or to track progress from year to year.	Responsible Official phone:	

Appendix F Survey Instrument

Q33 Thank you for taking time to answer this survey. The survey has 28 statements. You will be asked to register your opinion on a scale of "Strongly Agree" to "Strongly Disagree". I estimate 15 minutes is required to complete the survey. If you should have to interrupt answering the survey, you may resume by clicking the link in the email which invited you to participate. You will have an opportunity to check your work when you finish. If you have any questions, please email JimFlowers@gsu.edu or call him at 678 466 4316.

TM1 On the campus, deans, vice presidents, department chairs, and unit managers consider information security an important organizational priority.

- ❍ Strongly Disagree (1)
- ❍ Disagree (2)
- ❍ Neither Agree nor Disagree (3)
- ❍ Agree (4)
- ❍ Strongly Agree (5)

TM2 The institution's cabinet members are interested in security issues.

- ❍ Strongly Disagree (1)
- ❍ Disagree (2)
- ❍ Neither Agree nor Disagree (3)
- ❍ Agree (4)
- ❍ Strongly Agree (5)

TM3 University management takes security issues into account when planning university strategies

- ❍ Strongly Disagree (1)
- ❍ Disagree (2)
- ❍ Neither Agree nor Disagree (3)
- ❍ Agree (4)
- ❍ Strongly Agree (5)

TM4 The words and actions of senior management demonstrate that security is a top priority

- ❍ Strongly Disagree (1)
- ❍ Disagree (2)
- ❍ Neither Agree nor Disagree (3)
- ❍ Agree (4)
- ❍ Strongly Agree (5)

TM5 Visible support for security goals by senior management is obvious

- ❍ Strongly Disagree (1)
- ❍ Disagree (2)
- ❍ Neither Agree nor Disagree (3)
- ❍ Agree (4)
- ❍ Strongly Agree (5)

TM6 Senior management gives strong and consistent support to the security program.

- ❍ Strongly Disagree (1)
- ❍ Disagree (2)
- ❍ Neither Agree nor Disagree (3)
- ❍ Agree (4)
- ❍ Strongly Agree (5)

UT1 Necessary efforts are made to educate employees/students about new security policies

- ❍ Strongly Disagree (1)
- ❍ Disagree (2)
- ❍ Neither Agree nor Disagree (3)
- ❍ Agree (4)
- ❍ Strongly Agree (5)

UT2 On the campus, information security awareness is communicated well

- ❍ Strongly Disagree (1)
- ❍ Disagree (2)
- ❍ Neither Agree nor Disagree (3)
- ❍ Agree (4)
- ❍ Strongly Agree (5)

UT3 On the campus, a variety of communication media (notices, posters, newsletters, etc.) are used to promote security awareness

- ❍ Strongly Disagree (1)
- ❍ Disagree (2)
- ❍ Neither Agree nor Disagree (3)
- ❍ Agree (4)
- ❍ Strongly Agree (5)

UT4 On the campus, an effective security awareness program exists

- ❍ Strongly Disagree (1)
- ❍ Disagree (2)
- ❍ Neither Agree nor Disagree (3)
- ❍ Agree (4)
- ❍ Strongly Agree (5)

UT5 On the campus, a continuous, ongoing security awareness program exists

- ❍ Strongly Disagree (1)
- ❍ Disagree (2)
- ❍ Neither Agree nor Disagree (3)
- ❍ Agree (4)
- ❍ Strongly Agree (5)

UT6 On the campus, Users receive adequate security refresher training appropriate for their position (student, faculty, staff, etc).

- ❍ Strongly Disagree (1)
- ❍ Disagree (2)
- ❍ Neither Agree nor Disagree (3)
- ❍ Agree (4)
- ❍ Strongly Agree (5)

SC1 On the campus, employees/students value the importance of security

- ❍ Strongly Disagree (1)
- ❍ Disagree (2)
- ❍ Neither Agree nor Disagree (3)
- ❍ Agree (4)
- ❍ Strongly Agree (5)

SC2 On the campus, a culture exists that promotes good security practices

- ❍ Strongly Disagree (1)
- ❍ Disagree (2)
- ❍ Neither Agree nor Disagree (3)
- ❍ Agree (4)
- ❍ Strongly Agree (5)

SC3 On the campus, security has traditionally been conisdered an important

organizational value

- ❍ Strongly Disagree (1)
- ❍ Disagree (2)
- ❍ Neither Agree nor Disagree (3)
- ❍ Agree (4)
- ❍ Strongly Agree (5)

SC4 On the campus, practicing good security is the accepted way of doing business

- ❍ Strongly Disagree (1)
- ❍ Disagree (2)
- ❍ Neither Agree nor Disagree (3)
- ❍ Agree (4)
- ❍ Strongly Agree (5)

SC5 On the campus, the overall environment fosters security minded thinking

- ❍ Strongly Disagree (1)
- ❍ Disagree (2)
- ❍ Neither Agree nor Disagree (3)
- ❍ Agree (4)
- ❍ Strongly Agree (5)

SC6 On the campus, information security is a key norm shared by the universlty/college community

- ❍ Strongly Disagree (1)
- ❍ Disagree (2)
- ❍ Neither Agree nor Disagree (3)
- ❍ Agree (4)
- ❍ Strongly Agree (5)

PR1 On the campus, information security policy is consistently updated on a periodic basis

- ❍ Strongly Disagree (1)
- ❍ Disagree (2)
- ❍ Neither Agree nor Disagree (3)
- ❍ Agree (4)
- ❍ Strongly Agree (5)

PR2 On the campus, Information security policy is updated when technology changes require it

- ❍ Strongly Disagree (1)
- ❍ Disagree (2)
- ❍ Neither Agree nor Disagree (3)
- ❍ Agree (4)
- ❍ Strongly Agree (5)

PR3 On the campus, policy is updated when legal & regulatory changes require it

- ❍ Strongly Disagree (1)
- ❍ Disagree (2)
- ❍ Neither Agree nor Disagree (3)
- ❍ Agree (4)
- ❍ Strongly Agree (5)

PR4 On the campus, an established information security policy review and update process exists

- ❍ Strongly Disagree (1)
- ❍ Disagree (2)
- ❍ Neither Agree nor Disagree (3)
- ❍ Agree (4)
- ❍ Strongly Agree (5)

PR5 On the cap,us, security policy is updated on a regular basis

- ❍ Strongly Disagree (1)
- ❍ Disagree (2)
- ❍ Neither Agree nor Disagree (3)
- ❍ Agree (4)
- ❍ Strongly Agree (5)

PR6 On the campus, information security policies are aligned with university/college goals

- ❍ Strongly Disagree (1)
- ❍ Disagree (2)
- ❍ Neither Agree nor Disagree (3)
- ❍ Agree (4)
- ❍ Strongly Agree (5)

PR7 On the campus, information security policies reflect the objectives of the university/college

- ❍ Strongly Disagree (1)
- ❍ Disagree (2)
- ❍ Neither Agree nor Disagree (3)
- ❍ Agree (4)
- ❍ Strongly Agree (5)

PR8 On the campus, risk assessments are conducted prior to writing new security policies

- ❍ Strongly Disagree (1)
- ❍ Disagree (2)
- ❍ Neither Agree nor Disagree (3)
- ❍ Agree (4)
- ❍ Strongly Agree (5)

PE1 On the campus, employees/students caught violating important security policies are appropriately corrected

- ❍ Strongly Disagree (1)
- ❍ Disagree (2)
- ❍ Neither Agree nor Disagree (3)
- ❍ Agree (4)
- ❍ Strongly Agree (5)

PE2 On the campus, information security rules are enforced by sanctioning the employees/students who break them

- ❍ Strongly Disagree (1)
- ❍ Disagree (2)
- ❍ Neither Agree nor Disagree (3)
- ❍ Agree (4)
- ❍ Strongly Agree (5)

Q32 You have complete the survey. If you wish to review your answers -- click the back button (<<). If you are done, click (>>).You may contact Jim Flowers at 678-466-4316 or jimflowers@gsu.edu if you have questions/comments.Thank you for your time!

Appendix G Interview Protocol

Interview Protocol

Below is a list of positions of interest in this study. Interview subjects will be selected on two criteria: a) basis of position within the primary action situation, or b) identified by an actor in the primary action situation as a primary actor within a networked adjacent action situation. Given that actors in adjacent action situations are likely non-technical, the interview protocol will be adjusted to reflect the role their actions played in the decision process.

As individuals note participants relative to decision making regarding the policy process, those participants may be added to the list to be interviewed. The method is a modified structured snowball approach. It is structured by the requirement that a participant will be interviewed only if they contribute directly to the outcome of a network adjacent action situation which has direct effect upon the outcome of the action situation which governs implementation of security policy.

Likely Actors to be Interviewed

- Chief Information Officers
- Chief Information Security Officers
- Finance and Administration
- Executives (Deans, Provosts, Presidents) – if identified as participants by implementation group
- Audits
- Risk Management Project Managers

Scope of this version of the Instrument

This interview protocol contains most of the themes we may be interested in when interviewing actors of interest

Reminders

1. Before conducting interviews, read our research purpose and research questions again.
   a) Research Question

      This study proposes to how the rule governing the decision making process for cyber security vary from one institution to another. .
2. Don't need to follow the sequence of questions outlined in the protocol. Adjust your order of questions based on the answers of interviewees.
3. Pay particular attention to those important questions (***) in the protocol. Try to use different ways to get the answers to them.
4. Adjust your interviewing style and questions to keep the conversation going in a way that keeps the attention and interest of the interviewees on the topic of the question. But
5. If the interview is terminated early, ask for call back privileges.
6. Let the interviewee do the talking.

Interview Data Form

Background Information on Interviewee

Date and Time of Interview:

Location of Interview:

Name:

Job Title:

Job Responsibilities:

Organization:

Email:

Telephone:

Begin with:

i. Request interviewee to sign IRB informed consent form
ii. Request to tape record
iii. Explain role of second interviewer (if present)
iv. Exchange business cards
v. Brief introduction of our research topic. For example:

Semi-structured interview Protocol for Actors in primary Action Situation

Part I Identification

These questions will identify the participant, and "warm up" the interview

1) Contact info : Name, Phone, email
2) Title
3) To what position and whom do you report?
4) What was your prior position/institution?
5) What is your role in implementing cyber security policy?
6) What is your position in creating/adopting cyber security policy?

Part II Exogenous Data

Questions will validate some survey elements, and "warm up" the interview

Environmental

Do you have a budget for cyber security?

If so, how much?

What kind of technology do you use to monitor and enforce security policies?

i. Are there allocations for security in other budgets within your organization?
ii. What are the requirements for admitting someone to the decision making process for cyber security? Who set those requirements?

Community

Is there an awareness regarding security?

How does the community respond to security policies?

What is the biggest challenge you face in implementing cyber security policy?

What is the biggest challenge you face in developing policy?

Part III Action Situation Data

Policy Process

2. How are cyber security policies created?
    a. (Actors) Who must review new/modified/deleted policies?
        i. What are their titles?
        ii. What position do they usually advocate? (enforcement, standards, more tech, etc)
        iii. Do they participate in all of the discussions?
        iv. What are the requirements for admitting someone to the decision making process for cyber security? Who set those requirements?
        v.
    b. Rules
        i. Is there a formal process for reviewing, developing, adopting security policy? (If so, are those rules available in written form?)
3. Were there policies you wished to implement, but were unable to do so? (**Probe**: discover who, what, when) If so, why were you unable to implement? **Probe**: Did you learn about this policy from another source(s)?

Boundary

1. Who decided the make-up of the decision/implementing group?
2. Who participated in this group?
3. Was there a time when others joined the implementation group? If so, when? Who made the decisions as to who might leave or enter the group?

Position

4. What position did you occupy in the decision making for implementation? (e.g. chair, leader)
5. What were the other positions/what was the structure of the decision making/implementing group? Who occupied those positions?

Information

6. What were the sources of information? Who provided the information?
7. Were there external organizations that influenced the policies implemented here? If so, which organizations?

Choice

8. Who set the agenda? How was the agenda determined? Could anyone affect that agenda?
9. When was the current version of security policy implemented?
10. Were there limits placed as to what could be implemented? By whom?
11. What were the budgetary constraints? Who decided the level of those constraints?

Aggregation

12. How did the decision-making process work with regards to the policy creation/adoption decisions? (**probe** here – let the interviewee tell the story. Follow up for data per questions below)
13. What are the rules used to decide what and how to implement security policy?
14. Who /what positions were needed at the table to make those decisions?
15. Did any one position or person have more weight than another in the process?

Scope

16. What was the initial scope of the policy?
17. Are there areas of the campus where these security policies may not apply? If so, who makes those policies?
18. Were there any ground rules, written/informal, that were used as criteria for determining to whom/what the policy would be applied/enforced? Who set those criteria?

Payoff

19. Was the incentive/mandate from an outside group? If so, whom?
20. How were costs/benefits calculated? Were they calculated?
21. Did anyone require costs/benefits analysis as part of their support for policy change? If so, whom?

Ending the Interview

If you could make any changes in the process for implementing/deciding security policy,

what would those changes be?

Is there anything else you would like to say?

Thank you for your time.

Appendix H Institutional Analysis Protocol

Summary

When all of the case data is collected, and the meta-data summarizing each document is complete, then we may begin identifying the statements and assigning values to the variables of interest. The data entry process is supported by a script written in Microsoft Access. A screenshot (Figure H-1) illustrates what a "disassembled" statement will look like when the process is complete.

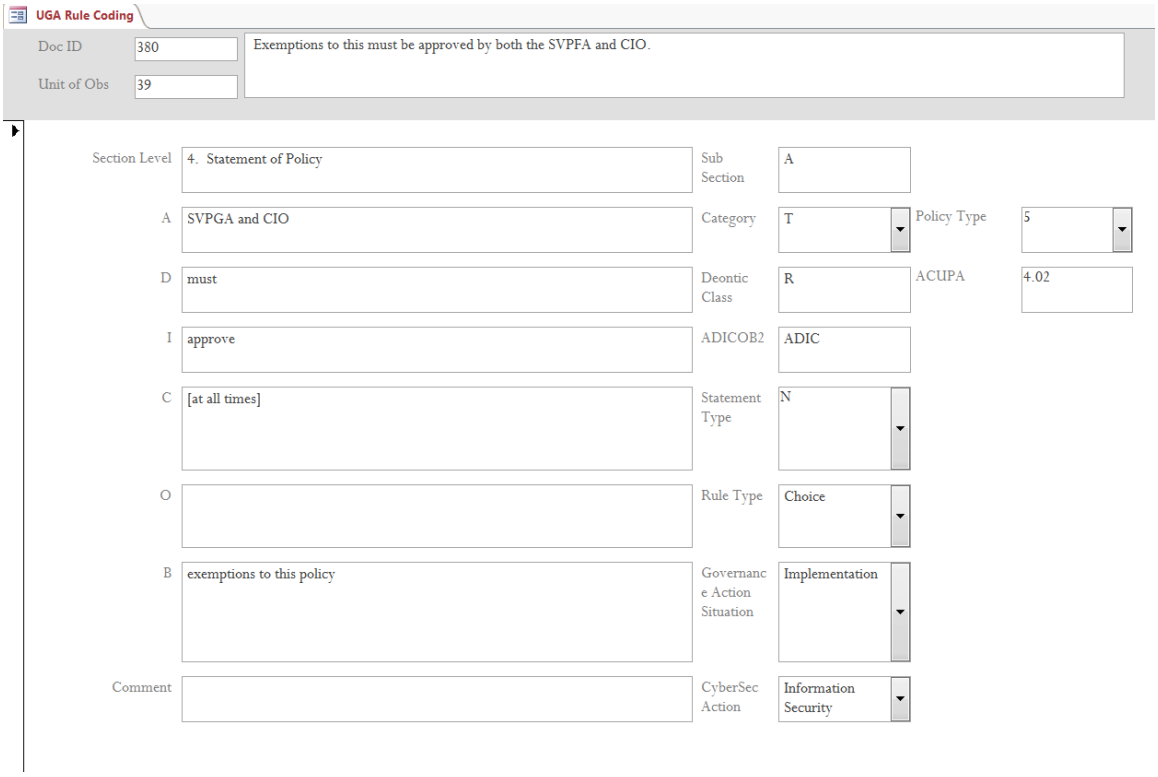

Figure H-1 Data Entry of Disassembled Statement

Identifying institutional statements

Treat each sentence of a policy document as a unit of observation. The sentence is given a unique identity number. The statement seen in Figure H-1 is assigned the identifier 376:32. Simply interpreted, the statement is the 32nd observation found in document number 376 (UGA's Data Access Policy).

Each statement is broken into its distinct components using the process adapted from Basurto, et al (2009, pp. 4-6) and Siddiki, et al (2011). The process differs from that of prior studies as it maintains all statements, including titles, preambles and headings so that document structure is preserved. Instead of discarding these

statements, they are coded as “O” for an Outline indicator per suggestions found in Basurto, et al (2010).

The analysis requires the following steps:

1. Subdivide all initial section or subsection units from step 2 that have multiple sentences into sentence-based units of observation. If a section of subsection does not have a complete sentence ending in a period, code the entire section or subsection as one unit of observation. If there are multiple sentences in the section of subsection, code each sentence as units of observation.
2. Break the unit of observation into the components defined by the ADICO syntax.
3. Code the **Attribute Category** as an Organization, Individual, Top Management, or vendor. These values categorize the responsible entity for following the direction of the institutional statement (Table H-1). Values are used to summarize who participates in an action situation.

Table H-1

Category	**Code**	**Definition**
Individual	I	A student, staff member, or faculty member. Also visitors and other persons referenced as themselves and not as a paid position within the organization.
Organization	O	Attribute refers to the organization, or any of its subunits
Top Management	T	In the context of USG, top management is a position of director or above. Includes CIO, IT Director, security officer, Assoc. Vice Presidents, VP’s, President
Vendor	V	Any third party organization not a subdivision of the case or USG.

4. Assign the statement to a **policy component**.
   Policy Type is discussed as policy components in chapter 3. Policy type is the nomenclature used by Doherty, et al. (2009).

Table H-2 Policy Components

Components of Technology Plans		
Policy Level	**Policy Component**	**Definition**
0	Ancillary	A placeholder for any statement that does not fit other definitions
1	Guideline	suggestion, approach, or issue that the attribute should consider when undertaking a defined activity (policy making, implementing)
2	Procedure	a specific instruction which must be followed in order to comply with prescribed policies and practices (Moule & Giavara, 1995)
3	Standard	Lower level policy - Established rules or requirements that must be observed in execution of procedures (Baskerville & Siponen 2002)
4	Policy	High level info sec policy - defines mgt and employee responsibility to preserve resources (Baskerville & Siponen 2002)
5	Metapolicy	Establishes how info sec policies are created, implemented, enforced (Baskerville & Siponen 2002)

5. Assign the **Deontic Class**. The institutional statements are coded for Deontic Class as defined by Crawford and Ostrom (2005a; 1995). The aIm verb served as the key means of identification.

   To make comparison easier and more reliable, the observed deontics were categorized into classes defined as permissive (P), required (R), and forbidden (F). Normative statements using a form of the verb should are coded as (S). This coding scheme is consistent with that employed by Ostrom and Basurto (2011) and aids in the construction of tables displaying rule configurations

Table H-3 Deontic Classification

Value	**Code**	**Definition**
Required	R	Verb forms of Shall, Must, will – indicate a required actions
Permitted	P	Verb forms of may, should, can – indicate an action is permitted, but not required.
Forbidden	F	Verb forms of may not, shall not, must not, cannot --

6. **If the Policy Type = 5 (A Meta-policy)** - Assign the statement to the appropriate **ACUPA Step**.

Several IAD researchers have proposed a "nested analysis" approach to analyzing the structure of action situations (Basurto et al. 2010a; S. Siddiki, Basurto, and Weible 2010). Basurto, Kingsley, et al., suggested that a research could sort their observations into "common sections and subsections that share the same broad aim" (2010a, 528). The ACUPA model is a practical guide to link the observations as the cases studied relied on the ACUPA steps to inform their practices. With the data divided, I applied the configuration method (E. Ostrom and Basurto 2011) to analyze the structure within each ACUPA action set.

ACUPA steps are meta-policy processes. This code applies only to statements of the policy type (class) "Meta-Policy", value of (5). Align the action of each statement within the criteria. The alignment of these steps with Knapp Processes may help (Table H-4).

Table H-4 Alignment of ACUPA Steps to Knapp Action Situations

Action Situation	Action #	Actions	Knapp Action
1. Identify Issues	.01	Scans for changes in law, threat, best practices, organizational change, technology change, need to control risky behavior	Risk
	.02	may identify need/issue	Development
2. Conduct Analysis	.01	Identify Owners	Development
	.02	Determine Path (Policy Plan – Scope Definition)	Development
	.03	Assemble Team	Development
	.04	Gather Data	Development
	.05	Id deadlines	Development
	.06	Determine Risks	Risk
	.07	Determine Stakeholders	Development
	.08	Determine solutions for the problem/need	Development
	.09	Determine if present policy can be revised	Development
	.10	Determine need for new policy	Development
3. Draft Policy	.01	Agree on Definitions	Development
	.02	Drafts Policy -Use Common Format	Development
	.03	presents drafts to stakeholders	Development
	.04	review and vet proposals	Development
	.05	presents to policy advisory Committee	Development
4. Get Approvals	.01	Presents policies for approval to advisory committee	Approval
	.02	Considers/approves/modifies proposals	Approval
	.03	collects comments/revises as needed	Approval
	.04	Obtain Approvals	Approval
5. Education (Awareness)	.01	Plan Communications	Awareness
	.02	Put online	Awareness
	.03	Provide searches	Awareness
	.04	Communicates policy to appropriate audiences	Awareness
6. Plan Maintenance (Review/Risk Assessment)	.01	Versions new policy	Maintain
	.02	Archives old poicy	Retirement
	.03	Establishes schedule for review	Review
	.04	Determines review procedures	Review
	.05	solicits feedback	Review
	.06	Reviews risk and Cost	Risk
	.07	Recommends whether policy still needed	Review
7. Measurement & Compliance	.01	Measures/monitors outcomes	Monitor
	.02	Enforcement	Enforcement

Enter the **ADICOB2** sequence represented by the grammatical components observed in the statement. The coding scheme offered by Basurto et al. (2010) is used to identify institutions by type (Strategy, Norm, Rule) within a policy and to investigate the effects of the institutional type on policy outcomes (Nowlin 2011)[48]. The statements are coded based upon the presence of ADICO elements as follows:

AIC	**S**trategies
ADIC	**N**orms
ADICO	**R**ules

Ex: If no deontic is present, but an Attribute, aIm, and Condition are present – code is AIC. If a deontic were present – ADIC.

An institutional statement is composed of:

Table H-5 Institutional Statement Components

Grammar Component	Code	Definition
Attributes		a variable which identifies the actor, or position, to whom the statement applies
Deontic		a variable which contains the modal verb defining what may be permitted, required, or forbidden.
a**I**m		variable describing the actions or outcomes to which the deontic is assigned. The action or outcome must be physically possible. The negation of the action or outcome must be possible as well.
Conditions		a variable defining when, where, how and to what extent the aIm is allowed per the Deontic
Or else		a variable defining the sanctions to be imposed for not following the rule.
o**B**ject		separates those responsible for carrying out the aIm from those receiving the aIm (S. Siddiki et al. 2011, 87)

[48] There are challenges in determining the type of institution being observed by the analyst. (See notes on Schluter, and Basurto, and Crawford and Ostrom). This study employs a strategy used by Siddiki et al. (2010):

> *In the original grammar tool (Crawford and Ostrom, 1995), this increasingly stringent ordering of categories of institutional statements corresponded with "strategies" (AIC), "norms" (ADIC), and "rules" (ADICO). In this paper, we recognize the underlying logic of ordering the statement categories by stringency from strategies to rules. But we avoid using the conceptual language of strategies, norms, and rules because all statements in formal institutions could be interpreted as rules. More important than the actual label applied is the relative frequency of each categorization and the understanding such categorization provides into the content of the policy documents.*

7. Assign an institutional **statement type**. Code the observation as rules, norms or strategies (Table H-6). A rule has all ADICO components. A norm has ADIC components. And a strategy has AIC components. If not an institutional statement, code the statement as appropriate.

Table H-6 Statement Type Definitions

ID	Statement Type	Statement Name	Description
1	S	Strategy	Has AIC components
2	N	Norm	Has only ADIC components
3	R	Rule	Has all ADICO components
4	D	Definition	Statement defines a term, attrrbute, or AIM
5	E	External Policy Reference	references or provides a reference to an external policy document
6	O	Outline Indicator	A section title
7	B	Objective = defines the objective of the policy	describes the policy objectives

Coding the institutional statements is essential to efficiently analyzing the data. However, many "non-institutional" statements (NI), provide important meaning for institutional statements. I chose to catalog these statements for the following reasons. First, by identifying and classifying the observations as NI, the reliability of the coding process may be enhanced as each statement is included in the inventory. Researchers may understand why a statement was included, and why a statement was not included. Second, some definitions and external document references are important to understand the "combinatorial" effects of institutions thought important by Ostrom. These effects are confirmed by authors who observe that cyber security policies must be consistent with organizational culture and business objectives (Knapp et al. 2009). An effective combination of institutions regarding the identification of risk, the assessment of policy effectiveness, and the means of making users aware of policies is needed (Baskerville & Siponen, 2002).

Third, within institutional statements, some components are implied, or referenced. I enclosed implied/referenced text with square brackets [example text]. The NI statements also provide both meaning and context to these implied components. Crawford and Ostrom note that the existence of single institutional statements, independent of all other statements relevant to a policy document, is not easily found in the real world (1995, 596). NI statements provide links to other stated deontics, conditions, and sanctions (Or Else components). Such links are observed by Basurto, et al (2009) and deemed important to understanding the correct meaning of policy documents (p. 14).

For example, Georgia State University publishes a policy document (ID 361) entitled "University Information Systems Use Policies". The meta-data for the document indicate that it is a Policy, of type "Acceptable Use" containing 587 words broken into 22 sentences. Applying the IGT to the document, we discover only one rule and 8 norms leaving 13 Non-Institutional statements (Table H-7).

Table H-7 Sample Analysis of Statement Types

Statement Type	**Units of Observation**
Standard	0
Norm	8
Rule	1
oBjective	1
Definition	11
External Policy Reference	1
Total	22

A display of the institutional statements is found in Table H-8. Examination of these few statements demonstrates the importance of implicit links to sanctions, conditions, and attributes which are contained in other institutions within the organization's policy apparatus.

Observation 18 says that disciplinary procedures and sanctions are described in detail in the "Faculty Handbook, the Student Code of Conduct, and other applicable policies and procedures." These references to policy documents external to this particular policy is a good example of the combinatorial nature of institutions of which studies like this one must be aware. When an observation makes such a reference, the references are recorded and the components of security governance documented. The referenced documents' meta data are captured in the same manner as meta data for the cyber security policy documents under study.

Table H-8 Sample Display of Institutional Statements

Unit of Obs	Text	Deontic Class	Statement Type
13	Violations of these policies may result in the discipline of an individual in accordance with applicable University policies or state or federal law, including criminal prosecution.	P	R
14	The university may temporarily suspend, block or restrict access to Information Systems when it reasonably appears necessary to do so in order to protect the integrity, security, or functionality of Information Systems or to protect the university from liability	P	N
15	Alleged violations of the policies should be reported to the appropriate university disciplinary and/or law enforcement authorities	O	N
16	If the alleged violation could pose a security hazard to the university's technology resources, the alleged violation should also be reported to the university's Information Security Officer for appropriate action to secure the affected technology resources	O	N
17	When appropriate, the university disciplinary and/or law enforcement authorities will coordinate with the university's Information Security Officer to investigate and respond to alleged violations.	O	N
18	Alleged violations of policies will be pursued in accordance with the appropriate disciplinary procedures for faculty, staff and students, as outlined in the Faculty Handbook, the Student Code of Conduct, and other applicable policies and procedures	O	N
19	Users found in violation of any of the catalogued policies may appeal any imposed disciplinary action in accordance with the appeals provisions of the relevant disciplinary procedures.	P	N
20	This document and any of the catalogued policies may be changed by the Information Technology Senate Sub-Committee (ITSS), with such changes being reviewed and recommended through the Senate Information Systems and Technology Committee (ISAT).	P	N
21	Information Systems and Technology (IS&T) will prepare, coordinate and process all recommended changes.	O	N

8. Assign a **rule type** to the statement. Use the definitions in Table H-9 to make the assignment

Table H-9 Rule Type Definitions

Rule Type	Description	Component	Basic Aim Verb
Position	Create the positions that actors hold. Title of position; Number of actors in a position; quorum level;	Position	Be
Boundary	Define (1) who is eligible to enter a position, (2) the process that determines which participants may/must enter positions, and (3) how a participant may/must leave. Some rules may spell out eligibility for participants	Actor	Enter or leave
Choice	what an actor must, must not, may, may not do based upon Conditions at the time of decision - Choice rules affect the total power created in an action situation Choice rules determine the decision tree linking actions to outcomes	Actions	Do
Aggregation	whether one individual decides, or votes of several aggregate to decide Determines the level of control an actor given a position may exercise over the selection of an action	Control	affect
Information	Affects level of information available to participants; limits topics to be considered; frequency and accuracy of communication, legitimate channels of communication, language	Information	Send or Receive
Payoff	Assigns external payoff/sanctions to particular actions Creates incentives and deterrents for action	Costs/Benefits	Pay or Receive
Scope	Defines the range of acceptable outcomes permitted. Also limits actions linked to the outcomes.	Outcomes	Occur
Source Ostrom and Crawford (2005, 191), annotated from definitions found in pages 188-213 and Ostrom and Basurto(2011).			

9. Assign the statement to a **governance action situation** using the Knapp processes as categories. The statements were coded as to which stage, action situation, of the Knapp model the statement was assigned. Again, the aIm verbs, with assistance from the oBject, helped to determine the proper action situation. In addition, the policy documents often declared the intended action situation with the statements that served as outline indicators.

Table H-10 Knapp Action Situation Definitions

Action Situation	Description
Approval	Actions required to approve policy; to operationalize the policy
Awareness and Training	Efforts to communicate to the campus community and to train them in the issues related to the policy in question
Development	Activities include issue identification, definition of scope, research and analysis and stakeholder input
Enforcement	Judgment of whether a violation of policy occurred; application of sanctions
Implementation	Operational level application of the rules and norms contained within the policy document
Monitoring	Observation of policy compliance, audits of systems, use of automated tools to scan for behaviors not allowed
Retirement	Removal of policy from active service
Review	Management review of policy performance, alignment with business objectives, and effectiveness given other emerging technologies and security issues
Risk Assessment	Identification of organizational values, policies that may be compromised if certain behaviors are allowed to occur

Observations are attached to specific Knapp processes by a combination of the context of the observation (document type and section heading) and the intent of the aIm verb and conditions.

10. Assign the statement to the **CyberSec Action** per the USG policy area identified. The requirement represents another level of analysis which can include many of the Knapp action situations focused on one policy issue.

Table H-11 USG Cyber Security Action Situations

ID	Action Situation	Description	References
1	Information Security Program	the USO, all USG institutions, and the GPLS shall create and maintain an internal information security technology infrastructure consisting of an information security organization and program that ensures the confidentiality, availability, and integrity of all USG information assets.	USG Info Sec Policy Section 11
2	HIPAA	To meet the requirements of the HIPAA Privacy and Security Rules, the University System of Georgia, it's institutions; hospitals, GPLS and benefit plans will develop policies, which govern the use and disclosure of PHI.	USG: Health Information - HIPAA Privacy and Security Policy Statement
3	Password	It is the responsibility of every Institution and the University System Office to implement authentication mechanisms such as passwords to access sensitive data and the responsibility of the user to appropriately select and protect their passwords.	USG Password Authentication Policy
4	AUP	The USG expects all institutions and their users to use IT resources in a responsible manner, respecting the public trust through which these resources have been provided, the rights and privacy of others, the integrity of facilities and controls, state and Federal laws, and USG policies and standards.	USG Appropriate Use Policy
5	Risk Mgt	University System of Georgia (USG) Institutions must ensure the confidentiality, integrity and availability of information and information systems resources and assets by protecting them from unauthorized access, modification, destruction, or disclosure and ensure the physical security of IT resources and assets.	USG Risk Management Policy
6	Continuity	This policy shall establish a requirement to develop a formal program to develop, maintain, and evaluate plans to appropriately respond to a wide range of contingencies and disasters that may occur at all of the USG institutions, System Office and Georgia Public Library Service.	USG Continuity of Operations Plan
7	Data Handling	This policy is intended to ensure that the information is uniformly used and disclosed in accordance with all USG policies and applicable state and federal laws.	USG Data Handling and Storage Policy
8	Incident	This policy establishes the requirement for each University System of Georgia (USG) institution and the University System Office (USO) to establish an internal capability for handling computer security incidents.	USG Computer Security Incident Management Policy
9	Cryptography	This policy establishes the requirement to use cryptographic controls on University System Office (USO) and University System of Georgia (USG) Institution information systems as necessary.	Use of Cryptography
10	Privacy	This Privacy Policy sets forth the University System of Georgia's ("USG") policy with respect to the gathering and dissemination of information we obtain from you on the web site for the University System of Georgia located at www.usg.edu ("Site").	Privacy Policy for www.usg.edu
11	Awareness	The USG's employees (full/part-time employees and contractors) shall be made aware of their basic information security responsibilities through an awareness program.	Security Awareness Program
12	Electronic Data Disposal	All computer systems, electronic devices and electronic media must be properly cleaned of sensitive data and software before being transferred outside of the University System or GPLS, either as surplus property or as trash.	Electronic Data Disposal
13	Copyright	The purpose of this guideline is to establish acceptable practices that support the policy as it applies to copyright violations.	Copyright Violation Guideline
14	Resource Management	Policies regarding appropriate, authorization and management of Institutional Resources	

11. **Comments**: Coder should assign any comments. If the statement is one of multiple statements disaggregated from one sentence, coder should note that the observation is the x statement of Y statements observed. In other words if 3 observations are found in one sentence and this observation is the second – note "2 of 3 observations".

Code institutional statements as strategies, norms, and rules

The coding scheme offered by Basurto et al. (2010) is used to identify institutions by type (Strategy, Norm, Rule) within a policy and to investigate the effects of the institutional type on policy outcomes (Nowlin 2011)[49]. The statements are coded based upon the presence of ADICO elements as follows:

AIC	**S**trategies
ADIC	**N**orms
ADICO	**R**ules

Coding the institutional statements is essential to efficiently analyzing the data. However, many "non-institutional" statements (NI), provide important meaning for institutional statements. I chose to catalog these statements for the following reasons. First, by identifying and classifying the observations as NI, the reliability of the coding

[49] There are challenges in determining the type of institution being observed by the analyst. (See notes on Schluter, and Basurto, and Crawford and Ostrom). This study employs a strategy used by Siddiki et al. (2010):

> *In the original grammar tool (Crawford and Ostrom, 1995), this increasingly stringent ordering of categories of institutional statements corresponded with "strategies" (AIC), "norms" (ADIC), and "rules" (ADICO). In this paper, we recognize the underlying logic of ordering the statement categories by stringency from strategies to rules. But we avoid using the conceptual language of strategies, norms, and rules because all statements in formal institutions could be interpreted as rules. More important than the actual label applied is the relative frequency of each categorization and the understanding such categorization provides into the content of the policy documents.*

process may be enhanced as each statement is included in the inventory. Researchers may understand why a statement was included, and why a statement was not included. Second, some definitions and external document references are important to understand the "combinatorial" effects of institutions thought important by Ostrom. These effects are confirmed by authors who observe that cyber security policies must be consistent with organizational culture and business objectives (Knapp et al. 2009). An effective combination of institutions regarding the identification of risk, the assessment of policy effectiveness, and the means of making users aware of policies is needed (Baskerville & Siponen, 2002).

Third, within institutional statements, some components are implied, or referenced. I enclosed implied/referenced text with square brackets [example text]. The NI statements also provide both meaning and context to these implied components. Crawford and Ostrom note that the existence of single institutional statements, independent of all other statements relevant to a policy document, is not easily found in the real world (1995, 596). NI statements provide links to other stated deontics, conditions, and sanctions (Or Else components). Such links are observed by Basurto, et al (2009) and deemed important to understanding the correct meaning of policy documents (p. 14).

For example, Georgia State University publishes a policy document (ID 361) entitled "University Information Systems Use Policies". The meta-data for the document indicate that it is a Policy, of type "Acceptable Use" containing 587 words

broken into 22 sentences. Applying the IGT to the document, we discover only one rule and 8 norms leaving 13 Non-Institutional statements (Table H-12 UGA Rule Types).

Table H-12 Sample UGA Rule Types

Statement Type	**Units of Observation**
Standard	0
Norm	8
Rule	1
oBjective	1
Definition	11
External Policy Reference	1
Total	22

Appendix I Source Documents for Meta Policy Observations

Org	Doc ID	Description	Observations (%)		Totals	Date Effective	Policy Objective
GS	332	AUP	2	2.9%		11-Nov-10	This Information Technology Appropriate Use Policy is authorized by the Board of Regents, Appropriate Use Policy (2009-014) which charges each University System of Georgia institution to develop policy that, at minimum, includes the Board policy guidelines. These guidelines establish that the institution and its users have an obligation to abide by the following standards of appropriate and ethical use:
GS	336	IT Policy Development & Review Process (Meta)	45	66.2%		1-May-10	This document describes the process and guidelines for developing and managing information technology related policies at Georgia Southern University.
GS	473	AGILE Development Principles	11	16.2%			
GS	474	GS Interview Analysis	10	14.7%			
		Total GS MetaPolicy Observations			68		
GSU	361	AUP	1	1.3%		24-Mar-06	A single location of approved policies aimed at ensuring that the access, use and protection of the Information Systems promote the university's objectives
GSU	367	InfoSec Mgt Security Policy (Meta)	21	26.6%		4-Mar-09	The University selected the Information technology -Security techniques -Information security management systems - Requirements (ISO 27001) as a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an Information

Appendix I Source Documents for Meta Policy Observations

Org	Doc ID	Description	Observations (%)		Totals	Date Effective	Policy Objective
							Security Management System (ISMS).
GSU	368	Network Security Standards	4	5.1%		6-Jan-04	The basic standards and guidelines described in this policy provide for the minimum acceptable environment for operating and accessing information systems.
GSU	371	Security Review Policy	4	5.1%		2-Nov-05	Where appropriate, information security personnel will conduct risk assessments of technologies/processes that are being evaluated and/or used at Georgia State University. The purpose of these assessments is to quantify the impact and probability of potential threats and vulnerabilities. Fu
GSU	470	GSU Interview	14	17.7%			
GSU	475	University Policy on University-Wide Policies	35	44.3%		7-May-08	This policy explains how policies that pertain to the whole university community are developed, approved and managed. The University Policy on University-Wide Policies is not binding on policies developed by individual colleges, schools, divisions or departments to govern their internal operations
		Total GSU MetaPolicy Observations			79		
GT	343	AUP	6	7.9%		1-Jul-05	It is the policy of the Institute that its IT resources be used ethically and legally, in accord with applicable licenses and contracts, and according to their intended use in support of the Institute's mission.

Appendix I Source Documents for Meta Policy Observations

Org	Doc ID	Description	Observations (%)		Totals	Date Effective	Policy Objective
GT	344	Data Access Policy	4	5.3%		2-Nov-05	The purpose of this policy is to provide a structured and consistent process for employees to obtain necessary data access for conducting Georgia Tech operations, defining the relevant mechanisms for delegating authority to accommodate this process at the unit level while adhering to segregation of duties and other best practices, as well as defining data classification and related safeguards.
GT	348	Credit Card Processing	2	2.6%		31-Jul-03	This policy provides requirements and guidance for all credit card processing activities for the Georgia Institute of Technology. At this initial publication of this policy the following sources were consulted and provided the basis for this program: ISO 17799, Visa CISP, MasterCard SDP
GT	353	InfoSec Exception Policy	18	23.7%		1-Jul-10	There will be times when business processes can and should take precedence over these policies. A review process is provided to approve and document requests for exemptions to Georgia Tech's security policies
GT	359	Policy Exception Procedure	1	1.3%		1-Jul-10	The process allows unit heads and Institute leadership to make an informed decision on whether or not to request an exception to a particular IT policy by understanding the risk and alternatives involved
GT	360	Policy Review Process (Meta)	34	44.7%		16-Jan-08	This document describes the process, also known as the Security Policy Review (SPR), which will be followed by OIT-IS when writing/revising security policies which will affect OIT and/or

Appendix I Source Documents for Meta Policy Observations

Org	Doc ID	Description	Observations (%)		Totals	Date Effective	Policy Objective
							Georgia Tech as a whole. This document is needed to provide the necessary guidance to write, review, and publish Security Policies, Standards, and Procedures in a timely and efficient manner.
GT	476	GT Interview Analysis	11	14.5%			
		Total GT MetaPolicy Observations			76		
UGA	376	Data Access Policy	1	1.4%		1-Jun-11	The University of Georgia (UGA) shall approve access to Sensitive Institutional Data in order to ensure that access to sensitive data is authorized, that sensitive data with a need for protection are used appropriately and that authorized access complies with the UGA Privacy Policy and relevant state and federal laws.
UGA	378	UGA Privacy Policy	1	1.4%		7-Jan-09	The purpose of this policy is to protect the privacy of individuals who have sensitive information stored (either in electronic or paper form) on assets owned by The University of Georgia, while at the same time providing the University the ability to share this information with authorized entities as required by policy or law.
UGA	380	Credit Card Processing	1	1.4%		22-Apr-11	This policy provides requirements and guidance for all credit and debit card processing activities for the University of Georgia, including UGA Athletic Department, Arch Foundation, and UGA Alumni Association.

Appendix I Source Documents for Meta Policy Observations

Org	Doc ID	Description	Observations (%)		Totals	Date Effective	Policy Objective
UGA	381	Network Security Standards	8	10.8%		1-May-05	This policy requires compliance with minimum security standards in order to help protect both individual devices and other devices connected to the UGA Network. Additionally, the policy is intended to prevent exploitation of university resources by unauthorized individuals
UGA	382	Password Policy	15	20.3%		N.A.	All UGA computing accounts shall be protected by strong passwords. Account holders and system administrators shall protect the security of those passwords by managing passwords in a responsible fashion
UGA	466	SecureGA Plan	4	5.4%		2-Apr-08	In 2007, Provost Mace and the Executive Management Team approved the campus-wide role based accountability model for protecting sensitive and critical data. The model is built on Process, People, and Technology. Only with sound best practices in each area can information security be truly effective.
UGA	471	Interview Analysis	23	31.1%			
UGA	472	UGA Security Committee Charter	21	28.4%		N.A.	Make recommendations to the Director of University Information Security and the Office of the CIO regarding information security strategy, policy, and the awareness and training program.
		Total UGA MetaPolicy Observations			74		
		Grand Total Observations			297		

Appendix J Georgia State Collective Level Observations

ACUPA	A	I	B	C	RULE TYPE	REF	DEONTIC
1.01	CISO	identify	need for policy	[at all times]	Choice	470 : 1	P
1.01	Data owners	identify	need for policy	[at all times]	Choice	470 : 2	P
1.02	Any member of the university community	initiate	the policy development process	although this role is typically performed by an administrative office,a Senate or Staff Council committee, a StudentGovernment Association committee,or an executive officer of the university.	Choice	475 : 1	P
2.01	The administrative office charged with implementing and overseeing the policy	be	the Responsible Office.	[at all times]	Position	475 : 3	R
2.01	The Information Security Officer (ISO), as designated by the Associate Provost for Information Systems and Technology,	develop	university information security policies	[at all times]	Position	368 : 50	R
2.02	University	implement	ISMS	incrementally and scaled in accordance with University requirements	Choice	367 : 3	R
2.03	CISO	select	team	to determine need for policy.	Choice	470 : 5	R
2.03	Policy owner	include	all relevant parties	in discussions and formulations.	Choice	475 : 2	P
2.03	The team	include	the Responsible Office.		Boundary	475 : 4	P
2.04	ISO	works	this material [standards, procedures and guidelines necessary to administer access to university information resources]	to develop in conjunction with information resource owners, the university data administrators and functional users	Aggregation	368 : 53	R

Appendix J Georgia State Collective Level Observations

ACUPA	A	I	B	C	RULE TYPE	REF	DEONTIC
2.06	information security personnel	conduct	risk assessments	Where appropriate, of technologies/processes that are being evaluated and/or used at Georgia State University	Choice	371 : 1	R
2.06	CISO and team	determine	costs	of implementing new policy	Choice	470 : 14	R
2.08	information security personnel	recommend	security controls	which, if any, are commensurate with the risks to which the university would be exposed.	Choice	371 : 3	P
2.09	Office of Legal Affairs	approve	the new policy	if umbrella policies cover the need.	Choice	470 : 7	F
2.09	[University]	develop and enact	an interim policy (and or procedures)	Where legal or compliance imperatives demand an immediate modification (or suspension) of policy (and practice), pending formal review and approval.	Choice	367 : 6	R
2.10	Office of Legal Affairs	approve	the draft	[at all times]	Aggregation	470 : 6	R
3.02	CISO	draft	draft policy	using approved format	Choice	470 : 13	R
3.02	Team	draft	policy	to present to key stakeholders	Choice	470 : 4	R
3.02	Team	use	the Policy Template	for all new policies and policy revisions	Choice	475 : 5	R
3.02	Office of Internal Audits	draft	policy	[at all times]	Choice	470 : 3	F
3.03	CISO	present	draft	to Internal Audits for comments	Information	470 : 9	R
3.03	CISO	present	draft policy	to CIO	Information	470 : 10	R
3.03	Team	revise	draft policy	accomodating comments by Office of Legal affairs	Choice	470 : 8	R
3.04	CIO	present	draft policy	to ISAT for examination and discussion if Legal approves and CIO approves	Choice	470 : 11	R
4.01	CIO	present	draft policy	to Admin Council	Information	470 : 12	R
4.01	[Team]	submit	policy drafts	to the Office of Institutional Effectiveness	Information	475 : 6	R
4.01	the Office of Institutional Effectiveness	arrange	the policy draft	to be reviewed by the Policy Advisory Group.	Choice	475 : 7	R
4.01	The Policy Advisory Group (PAG)	evaluate	proposed policy	(at all times)	Choice	475 : 9	F
4.01	The Policy Advisory Group (PAG)	review	drafts of policies	to ensure that all mandatory elements are completed, that format is consistent, and that any overlaps with policies or	Choice	475 : 8	R

Appendix J Georgia State Collective Level Observations

ACUPA	A	I	B	C	RULE TYPE	REF	DEONTIC
				conflicts with other policies or federal, state, or Board of Regents regulations are identified prior to its final approval.			
4.01	The provost	appoint	members	of the Policy Advisory Group	Boundary	475 : 10	R
4.02	Administrative Council	approve	new policies or revisions to existing policies	if administrative or operational policies	Choice	475 : 11	R
4.02	The Administrative Council	discuss	the proposed policy	if introduced to the council	Choice	475 : 30	R
4.02	the chair of that committee	be	sponsor of the proposed policy	when the policy is introduced in the Senate, If the drafted policy comes under the purview of the Senate Committee	Position	475 : 18	R
4.02	The Office of Institutional Effectiveness	be	[responsible office]	for overseeing the policy management process	Position	475 : 12	R
4.02	The Policy Advisory Group	review	drafts of new or revised policy	to (a) ensure that all mandatory elements are completed and consistency of format, and (b) identify any overlap with other policies or conflict with other policies or federal, state, and Board of Regents regulations.	Choice	475 : 15	R
4.02	The Policy Advisory Group	complete	reviews	in a maximum of 5 working days (urgent issues will be expedited).	Choice	475 : 16	R
4.02	The Policy Advisory Group	review	drafts of new or revised policy	to (a) ensure that all mandatory elements are completed and consistency of format, and (b) identify any overlap with other policies or conflict with other policies or federal, state, and Board of Regents regulations.	Choice	475 : 26	R
4.02	The Policy Advisory Group	complete	reviews	in a maximum of 5 working days (urgent issues will be expedited).	Choice	475 : 27	R
4.02	the relevant associate provost or vice president	be	sponsor of the proposed policy	if not [under the purview of the Senate]	Position	475 : 19	R
4.02	The Responsible Executive	[be]	sponsor	of the proposed policy when the policy is introduced in the Administrative Council.	Position	475 : 29	R
4.02	The Senate	pass or deny	the motion to approve	[at all times]	Aggregation	475 : 20	R
4.02	The Senate	discuss	the policy	when introduced	Choice	475 : 19	R
4.02	University Senate	approve	new policies or revisions to existing policies	if policy is academic or student related	Choice	475 : 11	R

Appendix J Georgia State Collective Level Observations

ACUPA	A	I	B	C	RULE TYPE	REF	DEONTIC
4.03	The Policy Advisory Group	return	the draft policy documents	to the Responsible Executive (e.g. vice president, associate provost) for introduction to the Administrative Council.	Choice	475 : 28	R
4.03	The Policy Advisory Group	return	draft policy document	to the Responsible Office/Senate Committee for scheduling the discussion of the policy on the University Senate Agenda.	Information	475 : 17	R
4.03	the Responsible Office	draft	the new policy or revision of existing policy.	With input from any interested parties and the relevant vice president or associate provost,	Choice	475 : 25	R
4.03	the Responsible Office and/or the relevant Senate Committee	draft	document containing the new policy or revises an existing policy.	With input from the relevant associate provost or vice president,	Choice	475 : 14	R
4.04	The Administrative Council	recommend	approval or denial	to the President	Aggregation	475 : 31	R
4.04	The President	concur or vetoe	the motion of the Senate	[at all times]	Aggregation	475 : 21	R
4.04	The President	deny or approve	the proposed policy.	when presented proposal by Administrative Council	Aggregation	475 : 32	R
4.04	the University Senate (academic and Student Policies) or the Administrative Council (administrative policies)	approve	All university-wide policies	prior to final approval by the President, as set forth in University Statutes.	Aggregation	475 : 13	R
5.02	[University]	make available	applicable documents	at points of use relevant versions	Information	367 : 9	R
5.02	The Associate Provost	post	the approved policy	on the University's policy website.	Choice	475 : 23	R
5.02	The Associate Provost	post	the approved policy.	on the University Website	Information	475 : 33	R
5.04	[Information Security Department]	make aware	All relevant personnel	of the relevance and importance of their information security activities and how they contribute to the achievement of the ISMS objectives	Information	367 : 27	R

Appendix J Georgia State Collective Level Observations

ACUPA	A	I	B	C	RULE TYPE	REF	DEONTIC
5.04	The Responsible Office or Senate Committee	notify	relevant individuals and departments	of the policy change.	Information	475 : 24	R
5.04	The Responsible Ofice	notify	relevant individuals and departments	of the policy change	Information	475 : 34	R
6.01	[Information Security Department]	include	A revision level showing the new document(s)/version(s)	When a new procedure, or version of a procedure, is issued for inclusion in the University's Information Security Management System	Information	367 : 10	R
6.01	[Information Security Department]	include	Point(s) of contact for questions or comments	When a new procedure, or version of a procedure, is issued for inclusion in the University's Information Security Management System	Information	367 : 11	R
6.01	[Information Security Department]	include	Date of last update or issuance	When a new procedure, or version of a procedure, is issued for inclusion in the University's Information Security Management System	Information	367 : 12	R
6.01	[Information Security Department]	include	Data classification (if sensitive or confidential)	When a new procedure, or version of a procedure, is issued for inclusion in the University's Information Security Management System	Information	367 : 13	R
6.03	[Information Security Department]	hold	meetings	for management reviews semiannually	Information	367 : 18	R
6.04	information security personnel	perform	security reviews	In these situations; to determine the threats, the likelihood of such events taking place, the estimated impact if they were to occur and recommend controls.	Choice	371 : 6	S
6.04	information security personnel	perform	security reviews	In these situations; to determine the threats, the likelihood of such events taking place, the estimated impact if they were to occur and recommend controls.	Choice	371 : 6	S
6.04	[Information Security Department]	include	Results of ISMS audits and reviews	in the management reviews	Information	367 : 19	R
6.04	[Information Security Department]	include	Feedback from interested parties	in the management reviews	Information	367 : 20	R
6.04	[Information Security Department]	include	Techniques, products or procedures, which could be used at the University to improve the ISMS's	in the management reviews	Information	367 : 21	R

Appendix J Georgia State Collective Level Observations

ACUPA	A	I	B	C	RULE TYPE	REF	DEONTIC
			performance and effectiveness				
6.04	[Information Security Department]	include	Status of preventive and corrective actions	in the management reviews	Information	367 : 22	R
6.04	[Information Security Department]	include	Vulnerabilities or threats not adequately addressed in the previous risk assessments	in the management reviews	Information	367 : 23	R
6.04	[Information Security Department]	include	Results from effectiveness measurements	in the management reviews	Information	367 : 24	R
6.04	[Information Security Department]	include	Follow-up actions from previous management reviews	in the management reviews	Information	367 : 25	R
6.07	Information Technology Senate Sub-Committee (ITSS)	change	This document and any of the catalogued policies	with such changes being reviewed and recommended through the Senate Information Systems and Technology Committee (ISAT)	Aggregation	361 : 20	P
6.07	Organizations that are within the scope of the University's ISMS	ensure	appropriateness of safeguards against security threats	[at all times]	Choice	367 : 29.2	R
7.01	[University]	conduct	Internal audits	of the ISMS at planned intervals at least annually	Choice	367 : 14	R
7.01	[Information Security Department]	maintain	ISMS records	unless specified othewise, in the department or college in which they were produced for a minimum of 30 days.	Choice	367 : 26	R
7.01	auditors	possess to enable them to act in accordance with the principles	personal attributes	[at all times]	Boundary	367 : 16	R

Appendix J Georgia State Collective Level Observations

ACUPA	A	I	B	C	RULE TYPE	REF	DEONTIC
		of auditing					
7.01	ISO	coordinates	standards, procedures and guidelines necessary to administer access to university information resources.	[at all times]	Aggregation	368 : 52	R
7.01	The Information Security Officer (ISO), as designated by the Associate Provost for Information Systems and Technology,	monitor	compliance with those policies and all applicable laws, rules and regulations	[at all times]	Choice	368 : 51	R

Appendix K GS Collective Level Observations

ACUPA	A	I	B	C	RULE TYPE	REF	DEONTIC
1.02	Anyone within the University community context	identify	Policy issues	[at all times]	Boundary	336 : 3	P
2.01	[an IT director]	be	Officer(s) of Coordinating Responsibility (OCR)	most of the time	Boundary	336 : 9	R
2.01	[an IT director]	be	Officer(s) of Coordinating Responsibility (OCR)	most of the time	Position	336 : 9	R
2.01	[CIO	be	Officer(s) of Primary Responsibility (OPR)	most of the time	Boundary	336 : 8	R
2.01	[CIO	be	Officer(s) of Primary Responsibility (OPR)	most of the time	Position	336 : 8	R
2.02	IT Directors	define	scope of the issue	[at all times]	Choice	336 : 5	R
2.02	Team	manage	the process	as the team decides	Choice	473 : 10	R
2.02	Team and stakeholders	receive	commendation	for maintaining pace of development	Payoff	473 : 8	R
2.03	CIO	invite	individuals	to become members of TASC	Boundary	474 : 6	R
2.03	Officer of Primary Responsibility	involve	subject-matter experts (SME's)	Once the Statement of Policy Need is created, as necessary	Boundary	336 : 13	R
2.03	Officer of Primary Responsibility	involve	Office of Legal Affairs and Internal Audit	Once the Statement of Policy Need is created, as necessary	Boundary	336 : 16	R
2.04	Officer of Primary Responsibility	gather	necessary information on the issue(s)	Once the Statement of Policy Need is created,	Choice	336 : 12	R
2.06	CISO, Legal Affairs, and office of internal audit	perform	risk assessment	on proposed policies and policy changes	Choice	474 : 9	R
2.07	Policy Owners	engage	stakeholders committed to sound policy development.	[at all times]	Boundary	473 : 5	R
2.07	IT Directors	determine	who is or should be affected by policy issue	[at all times]	Boundary	336 : 4	R
2.07	Stakeholders	include [be]	technical, management, and operational actors.	[at all times]	Position	473 : 4	R
2.09	IT Directors	determine	existence of policy	if policy exists	Choice	336 : 6	R
2.09	Officer of Primary Responsibility	review	related (pre-existing Georgia Southern) policies	Once the Statement of Policy Need is created,	Choice	336 : 14	R

Appendix K GS Collective Level Observations

ACUPA	A	I	B	C	RULE TYPE	REF	DEONTIC
2.09	Officer of Primary Responsibility	review	analogous policy(s)	Once the Statement of Policy Need is created, from peer institutions and/or best practices	Choice	336 : 15	R
2.10	each University System of Georgia institution	develop	policy	authorized by BOR Appropriate Use Policy (2009-14) that, at minimum, includes the Board policy guidelines.	Scope	332 : 3	R
2.10	IT Directors	deliver	Memoranda	regarding Statement of Policy Need	Information	336 : 10	R
2.10	Officer of Primary Responsibility	draft	Policy Concept Document	[once all the actions are completed]	Choice	336 : 17	R
3.01	CIO	determine	the period (time and frequency)	for students, employees, and service providers to re-affirm their recognition of this policy.	Aggregation	332 : 23.2	R
3.01	Team	simplify	policy	to minimize effort required to comply.	Choice	473 : 9	R
3.02	OCR	develop	initial draft policy and accompanying procedures	once input on the concept document has been obtained,utilizing the IT Policy templates to ensure consistency	Choice	336 : 28	R
3.02	Officer(s) of Coordinating Responsibility (OCR)	write	draft of the policy and operational procedures	Once input on the concept document has been obtained	Choice	336 : 24	P
3.02	OPR	determine	who will be responsible for drafting the policy and procedures	once input on the concept document has been obtained	Aggregation	336 : 27.1	R
3.02	OPR	determine	who will be responsible for drafting the policy and procedures	once input on the concept document has been obtained	Boundary	336 : 27.1	R
3.03	Officer(s) of Primary Responsibility (OPR) / Officer(s) of Coordinating Responsibility (OCR)	distribute	policy concept document	to all stakeholders	Information	336 : 19	R
3.03	Officer(s) of Primary Responsibility (OPR) / Officer(s) of Coordinating Responsibility (OCR)	solicit	input	from all stakeholders [regarding draft policy concept document]	Information	336 : 20	R

Appendix K GS Collective Level Observations

ACUPA	A	I	B	C	RULE TYPE	REF	DEONTIC
3.03	Officer(s) of Primary Responsibility (OPR) / Officer(s) of Coordinating Responsibility (OCR)	inform	stakeholders	[when distributing policy concept document] of possible changes to policies	Information	336 : 21	R
3.03	Officer(s) of Primary Responsibility (OPR) / Officer(s) of Coordinating Responsibility (OCR)	inform	stakeholders	[when distributing policy concept document] how it affects them	Information	336 : 22	R
3.03	Team	exchange	information	in face-to-face meetings as much as possible	Information	473 : 6	R
3.04	Information Technology Advisory Council	provide	feedback	on issues regarding instructional technologies	Choice	474 : 8	R
3.05	Team	receive	commendation	for maintaining progress by delivery of working policies	Payoff	473 : 7	R
4.01	Officer(s) of Primary Responsibility (OPR) / Officer(s) of Coordinating Responsibility (OCR)	present	draft policy	typically 30 days for consideration by President's Cabinet and relevant audiences	Information	336 : 31	R
4.01	Officer(s) of Primary Responsibility (OPR) / Officer(s) of Coordinating Responsibility (OCR)	present	draft policy	typically 30 days for consideration by President's Cabinet and relevant audiences	Information	336 : 31	R
4.03	Policy Owners	accept	stakeholder input	anytime in the cycle	Information	473 : 2	R
4.03	Policy Owners	satisfy	the stakeholders	through timely and continuous policy actions	Scope	473 : 1	R
4.03	Officer(s) of Primary Responsibility (OPR) / Officer(s) of Coordinating Responsibility (OCR)	make	revisions	as necessary, to draft policy	Choice	336 : 33	R
4.03	Officer(s) of Primary Responsibility (OPR) / Officer(s) of Coordinating Responsibility (OCR)	address	requests	for additional information, clarifications, objections, recommendations, etc.	Information	336 : 32	R
4.03	Policy Owner	revise	documents	documents upon feedback from advisory committees within 24-48 hours of feedback.	Choice	474 : 7	R

Appendix K GS Collective Level Observations

ACUPA	A	I	B	C	RULE TYPE	REF	DEONTIC
4.03	Team	deliver	viable policy drafts	frequently during the development process.	Information	473 : 3	R
4.04	OPR (CIO)	seek	policy approval	from President's Cabinet by submitting amended draft with date and version accordingly	Information	336 : 35	R
5.01	CISO	develop	awareness and training program	(at all times)	Choice	474 : 10	R
5.01	OCR	Develop	a communication plan / matrix	once input on the concept document has been obtained,for introducing the new policy	Choice	336 : 29	R
5.02	Officer(s) of Coordinating Responsibility (OCR)	post	the policy and procedures	to VPIT policy website Once approved,	Information	336 : 37	R
5.03	Officer(s) of Coordinating Responsibility (OCR)	post	approved policy	in master repository ensuring proper classification for easy reference	Information	336 : 40	R
5.04	Officer(s) of Coordinating Responsibility (OCR)	distribute	the policy and procedures	Once approved, according to the established communication plan	Information	336 : 39	R
5.04	Officer(s) of Coordinating Responsibility (OCR)	distribute	the policy and procedures	Once approved, according to the established communication plan	Information	336 : 39	R
5.04	Officer(s) of Coordinating Responsibility (OCR)	distribute	policy document	as per communication plan	Information	336 : 41	R
6.01	Officer(s) of Coordinating Responsibility (OCR)	date and version	[amended policy]	[at all times]	Choice	336 : 50	R
6.02	Officer(s) of Coordinating Responsibility (OCR)	create	a master backup	Once approved,	Choice	336 : 38	R
6.02	Officer(s) of Coordinating Responsibility (OCR)	Move	Retired/obsolete policy document	to a Policy Archive, ensuring correct classification to enable future reference	Choice	336 : 53	R
6.02	Officer(s) of Coordinating Responsibility (OCR)	Communicate	policy retirement	as per Communication Plan	Information	336 : 54	R
6.03	Officer(s) of Coordinating Responsibility (OCR)	review	the policy	periodically	Choice	336 : 44	R
6.04	CISO and Procurement	collaborate		in some instances to review policy	Choice	474 : 3	R
6.04	Officer(s) of Coordinating Responsibility (OCR)	oversee	policy implementation	[at all times]	Choice	336 : 42	R
6.04	TASC (Advisory committee)	review	policy changes	(at all times)	Choice	474 : 5	R

Appendix K GS Collective Level Observations

ACUPA	A	I	B	C	RULE TYPE	REF	DEONTIC
6.04	Team	review	the Policy Process	for effectiveness on a regular basis	Choice	473 : 11	R
6.06	CISO and Internal Audit Office	collaborate		to review risk	Choice	474 : 1	R
6.06	CISO and legal affairs office	collaborate		to review risk	Choice	474 : 2	R
6.06	Office of legal affairs	vet	policies	from a legal risk management perspective most of the time	Choice	474 : 4	R
6.06	Officer(s) of Coordinating Responsibility (OCR)	evaluate	policy	as per the review schedule specified in the policy itself	Choice	336 : 45	R
6.07	Officer(s) of Coordinating Responsibility (OCR)	determine		if policy ist still needed/applicable	Aggregation	336 : 46	R
6.07	Officer(s) of Coordinating Responsibility (OCR)	[determine]	new policy	due to extensive changes necessary? Is a new policy required	Aggregation	336 : 48	R
6.07	Officer(s) of Coordinating Responsibility (OCR)	amend, update, modify	[policy]	as necessary	Choice	336 : 47	R
6.07	Officer(s) of Coordinating Responsibility (OCR)	obtain	approval for changes	as required	Choice	336 : 49	R

Appendix L Georgia Tech Collective Level Observations

ACUPA	A	I	B	C	RULE TYPE	REF	DEONTIC
1.01	Information Security Office	meet	data stewards and/or policy owners	to scan for issues that need to be addressed by policy change	Information	476 : 3	R
2.00	PRC	provide	feedback and constructive criticism	for proposed OIT and GT Security Policies based on their respective functional areas.	Information	360 : 13	R
2.01	IS Policy and Compliance Manager (PCM)	kick off	process	when the IS Policy and Compliance Manager (PCM) receives the request to review a policy or write a new policy	Aggregation	360 : 22	R
2.01	IS Policy and Compliance Manager (PCM)	kick off	policy process	when the IS Policy and Compliance Manager (PCM) receives the request to review a policy or write a new policy.	Information	360 : 21	S
2.01	Georgia Tech's OIT Information Security (OIT-IS) group	develop	this policy	[at all times]	Choice	353 : 24	R
2.02	OIT-IS	follow	this process, known as Security Policy Review	when writing/revising security policies which will affect OIT and/or Georgia Tech as a whole.	Choice	360 : 2	R
2.03	GT Internal Audit	comprise	PRC	[at all times]	Boundary	360 : 10	R
2.03	GT Legal	comprise	PRC	[at all times]	Boundary	360 : 9	R
2.03	GT Registrar	comprise	PRC	[at all times]	Boundary	360 : 11	R
2.03	members from GT Legal, HR, OIT, Internal Audit, and Registrar	comprise	PRC		Boundary	360 : 5	R
2.03	OIT-ED	comprise	PRC	[at all times]	Boundary	360 : 7	r
2.03	OIT-EIS	comprise	PRC	[at all times]	Boundary	360 : 8	r
2.03	OIT-IS	comprise	PRC	[at all times]	Boundary	360 : 6	R
2.03	Technology/Service SME	comprise	PRC	[at all times] based on policy/standard	Boundary	360 : 12	R
2.07	PCM	seek	input	from the various technical communities on campus (GTITC, CSS, CSR's, while writing the new policy or updating existing policies	Information	360 : 27	R
2.08	PCM	perform	analysis	initial of the request	Choice	360 : 23	R

Appendix L Georgia Tech Collective Level Observations

ACUPA	A	I	B	C	RULE TYPE	REF	DEONTIC
2.08	PCM	document	changes	proposed (if a review) or proposed language (if a new request)	Choice	360 : 24	R
2.09	PCM	forward	information	to the OIT IS Director for preliminary approval to proceed.	Information	360 : 25	R
2.10	[GT organizations]	reduce	minimum requirements established in this policy	[in] Other policies, standards, procedures, and safeguards documents	Scope	343 : 14	F
2.10	[GT organizations]	augment	restrictions	for the sake of security [in] Other policies, standards, procedures, and safeguards documents	Scope	343 : 13	P
2.10	[GT]	submit	policy	to applicable federal and State statutes and regulations that guarantee either protection or accessibility of Institute records [will take precedence over this policy]	Scope	344 : 5	R
2.10	[GT]	submit	policy	to applicable federal and State statutes and regulations that guarantee either protection or accessibility of Institute records [will take precedence over this policy]	Scope	344 : 5	R
3.02	PCM	write	initial draft	Once approval from the OIT IS Director has been received, taking into account the edits from the OIT IS Director.	Choice	360 : 26	R
3.02	PCM	include	summary of proposed changes or new policy highlights	with the draft.	Information	360 : 29	R
3.03	PCM	send	initial draft	to the PRC for review.	Information	360 : 28	R
3.03	PCM	socialize	draft	with various groups (e.g. SGA, Faculty and Technical Leads) for feedback where appropriate	Information	360 : 30	R
3.04	CIO	vet	proposal	with executive leadership team	Information	476 : 1	P
3.04	Information Security Office	vet	proposal	with faculty excutive board, faculty senate, and all units of the campus	Information	476 : 2	R
3.04	Information Security Office	solicit	information	from campus units after proposal/need vetted with executive leadership	Information	476 : 4	R
3.04	Information Security Office	meet	associate dean and IT director for a campus unit	to discuss changes	Information	476 : 6	R
3.04	Information Security Office	vet	policy proposal	with HR, Legal Affairs prior to vetting with campus units	Information	476 : 11	R

Appendix L Georgia Tech Collective Level Observations

ACUPA	A	I	B	C	RULE TYPE	REF	DEONTIC
3.05	PRC	review	proposed changes	over a period not to exceed 1 month.	Choice	360 : 31	R
3.05	PRC	handle	initial discussion	During this time, over email with weekly face-face meetings as needed.	Information	360 : 32	R
3.05	PRC Members	are	input	expected to provide input based on their functional areas.	Information	360 : 33	S
4.01	PCM	keep apprised (or apprise)	PRC	of the discussions with the CIO and any changes that are proposed	Information	360 : 37	R
4.02	PRC	review	changes	Grammatical, format, or minor (e.g. contact information)	Scope	360 : 16	F
4.02	PRC	review	new policies, which will be written by OIT-IS	prior to CIO approval and policy publication	Choice	360 : 15	R
4.02	PRC Members	compile	final draft	At the end of 1 month, taking into account the various inputs and recommendations.	Choice	360 : 34	R
4.03	Information Security Office	meet	faculty senate committee	to review draft	Information	476 : 7	R
4.03	Information Security Office	present	final draft	to Faculty Executive Board prior to seeking approval.	Information	476 : 8	R
4.03	PCM	pass	approved PRC draft	to the CIO for approval.	Information	360 : 35	R
4.03	PCM	brief	CIO	on the proposed changes or new policy	Information	360 : 36	R
4.03	PCM	take	recommendations the CIO has	into account	Information	360 : 36.1	R
4.04	President of the Georgia Institute of Technology	[provide]	final approval of this policy	based on a review by the Information Security Policy Committee	Aggregation	348 : 8	R
5.01	The responsible university officer	notify via email and/or in writing	associate vice provosts; deans, associate vice presidents, unit heads, internal auditing, office of legal affairs, OIT information security, technical leads	upon approval of the policy and upon any subsequent revisions or amendments made to the original document	Information	343 : 187	R
5.02	[Institute]	publish	this policy	upon approval on the Georgia Tech website	Information	344 : 71	O
5.02	PCM	communicate	final document	via email to the campus, once the draft or changes have been approved	Information	360 : 38	R

Appendix L Georgia Tech Collective Level Observations

ACUPA	A	I	B	C	RULE TYPE	REF	DEONTIC
5.02	PCM	update and post	final draft	to the OIT Policy Website, once the CIO has approved the final draft	Information	360 : 39	R
5.02	The responsible university officer	publish on the Georgia Tech website	this policy	upon approval	Information	343 : 186	R
5.04	Georgia Tech Academic and Administrative units, including OIT,	communicate	this policy	to their users	Information	353 : 26	R
5.04	OIT-IS	notify	CIO	of the changes [grammatical, format, or minor] and publish them as necessary.	Information	360 : 17	R
5.04	OIT-IS	publish	this policy	upon approval	Information	353 : 29	R
6.01	Georgia Tech's OIT Information Security (OIT-IS) group	maintain	this policy	[at all times]	Choice	353 : 25	R
6.01	Georgia Tech's OIT Information Security (OIT-IS) group	maintain	this policy	[at all times]	Choice	353 : 25	R
6.03	OIT-IS, Internal Audit, and the Unit	review	approved exceptions	periodically	Choice	353 : 16	R
6.03	PRC	review	Security Policies/Standards/Procedures	on an annual basis, based on the initial publication date.	Choice	360 : 14	R
6.04	Georgia Tech Academic and Administrative units, including OIT,	submit	risk exception requests	via the approved process	Information	353 : 27	R
6.04	Georgia Tech Academic and Administrative units, including OIT,	submit	risk exception requests	via the approved process	Information	353 : 27	R
6.04	OIT-IS, Internal Audit, and the Unit	review	Any deviation from security policies and standards	via the Information Security Exception Review Process	Choice	353 : 13	R
6.04	the Georgia Tech Associate Vice President and Associate Vice-Provost for Information Technology.	change	The Computer & Network Security Policy and Procedures	by directive	Aggregation	343 : 184	P
6.04	The responsible university officer	change	this policy	[at all times]	Aggregation	343 : 183	P

Appendix L Georgia Tech Collective Level Observations

ACUPA	A	I	B	C	RULE TYPE	REF	DEONTIC
6.05	OIT-IS	notify	the following groups: OIT, Campus Deans and Chairs, Unit Business/Administrative Leads, Georgia Tech IT directors, ITAC, Campus CSR's, Internal Audit	via email and/or in writing upon approval of the standard and upon subsequent revision or amendments made to the original document	Information	353 : 30	R
6.05	OIT-IS, Internal Audit, and the Unit	require	the Unit Head, CIO, EVP, or Provost.	to approve exemption requests involving potentially significant risk to the Unit	Choice	353 : 17	P
6.05	OIT-IS, Internal Audit, and the Unit	involve	qualified information security professionals	in the exception review process	Boundary	353 : 14	R
6.05	OIT-IS, Internal Audit, and the Unit	log	all findings and results	in a central repository that is accessible to all Georgia Tech staff involved in the assessment of the exception request.	Choice	353 : 15	R
6.05	The responsible university officer	communicate	Any changes to the policy or procedures	promptly to the individuals and offices noted in section 8	Information	343 : 185	R
6.06	business processs	take precedence over	these policies [security policies and standards]	when there will be times	Choice	353 : 5	S
6.06	Information Security Office	do	internal risk assessments	annually	Choice	476 : 9	R
6.06	Information Security Office	contract	external risk assessments	every three years	Choice	476 : 10	R
6.06	OIT-IS, Internal Audit, and the Unit	approve	exception requests	that create significant risks without compensating controls	Choice	353 : 20	F
6.06	OIT-IS, Internal Audit, and the Unit	take into account	what value the exception will bring	to the Unit requesting the exception	Choice	353 : 19	R
6.06	OIT-IS, Internal Audit, and the Unit	evaluate	exception requests	consistently in accordance with Georgia Tech's risk acceptance practice	Choice	353 : 21	R
6.06	Unit	consider	what risks they may face by not adhering to the policy as well as the benefit gained by requesting the exception.	before doing so [requesting an exception]	Choice	359 : 2	S
6.06	we	consider	the security of Georgia Tech's infrastructure and data.	still	Choice	353 : 6	R
6.07	OIT-IS, Internal Audit, and the Unit	evaluate	exception requests	in the context of potential risk to the Unit and Georgia Tech as a whole	Choice	353 : 18	R

Appendix L Georgia Tech Collective Level Observations

ACUPA	A	I	B	C	RULE TYPE	REF	DEONTIC
6.07	Only he President of the Georgia Institute of Technology.	revise	this policy	by signature	Aggregation	348 : 78	P
7.00	Campus Units	supersede	institutional policy	with their policy.	Scope	476 : 5	F

Appendix M UGA Collective Level Observations

ACUPA	A	I	B	C	RULE TYPE	REF	DEONTIC
2.01	Information Technology Security Advisory Council	Develop	policy	when necessary, in accordance with Guidelines and Procedures for Blocking Network Access."	Choice	381 : 27	R
2.01	ITSAC	develop		[at all times]	Choice	382 : 26	R
2.01	Office of Information Security	write	minimum security standards for networked devices	[at all times]	Choice	381 : 23	R
2.01	The CIO and CISO	participate in development	policy	[at all times]	Boundary	382 : 28	R
2.01	CIO or CISO	identify	policy owners	for particular areas of concern	Boundary	471 : 1	R
2.01	the University of Georgia Information Security Committee	be	the name	of the committee	Position	472 : 3	R
2.02	Departments, units, or service providers	develop	stricter standards	for themselves with or without the advice or assistance of the CIO and CISO.	Scope	381 : 11	P
2.02	The CIO and CISO	produce	the policy plan	collaboratively	Choice	471 : 15.1	R
2.02	CISO	determine	likely path	in consultation with the CIO	Aggregation	471 : 2	P
2.02	The CISO and CIO	set	the agenda and scope	for policy development upon consultation with stakeholders.	Aggregation	471 : 14	R
2.03	Bursar's Office –	[be]	a member	of the University of Georgia Information Security Committee	Position	472 : 20	R
2.03	CISO	refine	the path, or strategies, taken to achieve policy change	in consultation with team members	Choice	471 : 3	p
2.03	Extended Campuses	[be]	a member	of the University of Georgia Information Security Committee	Position	472 : 17	R
2.03	Faculty & Research –TBD	[be]	a member	of the University of Georgia Information Security Committee	Position	472 : 16	R
2.03	Human Resources –	[be]	a member	of the University of Georgia Information Security Committee	Position	472 : 18	R
2.03	Internal Audit -	[be]	a member	of the University of Georgia Information Security Committee	Position	472 : 19	R

Appendix M UGA Collective Level Observations

ACUPA	A	I	B	C	RULE TYPE	REF	DEONTIC
2.03	ITMF -	[be]	a member	of the University of Georgia Information Security Committee	Position	472 : 15	R
2.03	Legal Affairs	[be]	a member	of the University of Georgia Information Security Committee	Position	472 : 13	R
2.03	Policy owners	be	individuals responsible for a business process, system or unit of the organization.	[at all times]	Position	471 : 1.1	P
2.03	Public Affairs	[be]	a member	of the University of Georgia Information Security Committee	Position	472 : 14	R
2.03	Team members	be	selected individuals	based on the issues and the areas of the university that are affected.	Position	471 : 4	p
2.03	the CIO, CISO, Office of Legal Affairs, the internal auditor, business process owners, and stakeholders selected by the CISO or CIO	be	members	of the team	Position	471 : 4	R
2.03	The CISO and CIO	select	managers whose area of authority is affected .	as team members	Boundary	471 : 9	P
2.03	The CISO and CIO	select	owners of a process or a system, affected by a perceived policy gap need	as team members	Boundary	471 : 8	R
2.03	The Office of Legal Affairs, Office of Internal Audit, Office of Finance, Office of Human Resources, Office of Public Affairs, and others named by the CISO	be	members	of the University Security Committee.	Boundary	471 : 20	R
2.04	Office of Legal Affairs	research	the legal obligations and risks posed to the university	as a liability or compliance issue, most of the time	Choice	471 : 11	R
2.04	team	gather	data	from subject matter expert(s), peer institutions that have similar policies, organizations like Educause, and other appropriate resources.	Choice	471 : 10	R

Appendix M UGA Collective Level Observations

ACUPA	A	I	B	C	RULE TYPE	REF	DEONTIC
2.06	UGA	employ	the ISO 31000 risk management framework	to analyze the risks, costs, and benefits	Choice	471 : 12	R
2.07	Management	identify	stakeholders	ad hoc	Boundary	471 : 7	P
2.07	stakeholders	be	groups that exist within the university organization		Position	471 : 5	P
2.07	stakeholders	be	individuals with an interest in the policy	if no formal organization responsible for that policy exists	Position	471 : 6	P
2.08	Departments, units, or service providers	develop	stricter standards	as needed	Choice	382 : 12	P
2.08	University of Georgia Information Security Committee	make	recommendations	to the Director of University Information Security and the Office of the CIO regarding information security strategy, policy, and the awareness and training program.	Choice	472 : 5	R
2.09	UGA	decide	to write or revise a new policy	only after examining the alternatives carefully.	Choice	471 : 13	R
2.10	UGA	develop	policy documents that may replicate the mandated policy	If a policy is required by an external organization	Choice	471 : 16	F
2.10	The CISO	make	final decision	as to scope and agenda for policy development activities.	Aggregation	471 : 15	R
2.10	the university	establish	policy	that defines responsibility of what needs to be done	Choice	472 : 27	R
3.01	ITSAC and OIS	responsible		for the accuracy of the subject matter	Aggregation	381 : 35	R
3.03	the CISO	socialize	the policy/issue and plan	with most of the affected parties during the drafting to help gain support for the policy change	Information	472 : 21	R
3.04	The Information Technology Management Forum (ITMF) Security Committee	provide	input	on “standards and policy development … involving the campus as a whole” .	Choice	472 : 22	R
3.04	The University Security Committee	make	policy recommendations	to the CIO and CISO	Choice	471 : 18	R
4.02	Office of Information Security	approve	exceptions to minimum security standards	[at all times]	Aggregation	381 : 24	R

Appendix M UGA Collective Level Observations

ACUPA	A	I	B	C	RULE TYPE	REF	DEONTIC
4.04	Departments, units, and individuals	request from the Chief Information Security Officer (CISO)	exemption	if unable to comply with the UGA Password Standard	Choice	382 : 13	R
4.04	ITSAC and the Offices of the CIO and CISO	approve changes to the UGA Password Standard		[at all times]	Aggregation	382 : 37	R
4.04	ITSAC and the Offices of the CIO and CISO	approve changes to the UGA Password Standard		[at all times]	Aggregation	382 : 37	R
4.04	Office of the CIO and the Chief Information Security Officer	final arbitration		for policy exception review	Aggregation	381 : 29	R
4.04	The UGA Office of Information Security	process through the Information Technology Security Advisory Council	the request for final approval	[at all times]	Choice	382 : 14	R
4.04	CIO	approve	draft policy	[at all times]	Aggregation	472 : 24	R
4.04	the President	approve	draft policy	[at all times]	Aggregation	472 : 25	R
4.04	the presidents cabinet	approve	draft policy	[at all times]	Aggregation	472 : 23	R
5.01	Policy Owners	develop	awareness activities	to inform stakeholders who will place the requirements into practice.	Choice	471 : 17	R
5.04	The Office of Information Security	provide	training	[at all times]	Choice	382 : 22	R

Appendix M UGA Collective Level Observations

ACUPA	A	I	B	C	RULE TYPE	REF	DEONTIC
6.03	ITSAC and OIS	review	policy	on an annual basis	Choice	381 : 34	R
6.03	[UGA}	update	this policy	as needed as card association regulations change	Choice	380 : 3	R
6.03	CISO, in cooperation with the ITMF-SECCOMM	review	the policy and standards	on an annual basis	Choice	378 : 45	R
6.03	CISO, in cooperation with the ITSAC	review	policy and standards	on an annual basis	Choice	382 : 35	R
6.03	CISO, in cooperation with the ITSAC	review	policy and standards	on an annual basis	Choice	382 : 35	R
6.03	The Office of Information Security	develop and review	this policy	on a regular basis	Choice	382 : 24	R
6.03	The Office of the Chief Information Officer, in cooperation with the University Security Committee	review	this policy	on an annual basis	Choice	376 : 32	O
6.04	ITSAC	participate in policy exception review		[at all times]	Boundary	382 : 27	R
6.04	Office of Information Security	develop and review	university-wide information security policy and procedures	[at all times]	Choice	381 : 22	R
6.04	The CIO and CISO	review	policy	[at all times]	Aggregation	382 : 29	R
6.04	The CIO and CISO	review	policy	[at all times]	Aggregation	382 : 29	R
6.04	The CIO and CISO	serve as the final arbitrators		in policy exception review	Aggregation	382 : 30	R
6.04	The CIO and CISO	serve as the final arbitrators		in policy exception review	Aggregation	382 : 30	R
6.04	The CIO and CISO	review	policy	[at all times]	Choice	382 : 29	R

Appendix M UGA Collective Level Observations

ACUPA	A	I	B	C	RULE TYPE	REF	DEONTIC
6.04	The CIO and CISO	review	policy	[at all times]	Choice	382 : 29	R
6.04	The Office of Information Security	participate in policy exceptions review		[at all times]	Boundary	382 : 25	R
6.04	[President]	review	development, execution and maintenance of UGA Security Plan	in concert with requirements of USG, state and federal mandates	Choice	466 : 27	R
6.04	The University Security Committee	review	policy	as needed	Choice	471 : 19	R
6.05	University of Georgia Information Security Committee	provide	critical analysis and feedback	on existing or proposed policies and initiatives related to information security and privacy to the Director of University Information Security and the Office of the CIO.	Choice	472 : 7	R
6.05	University of Georgia Information Security Committee	[provide]	Feedback and guidance	on development of a comprehensive IT Security Strategy encompassing people, processes and technology	Choice	472 : 9	R
6.05	University of Georgia Information Security Committee	[provide]	Recommendation	for improvement of Role-Based Accountability model and the University's information security training and awareness program	Choice	472 : 11	R
7.01	Departments	determine	how to comply with policy	in some cases.	Choice	472 : 28	P
7.02	[President]	[have] ultimate responsibility	for UGA Security Plan, policies, standards, and best practice	that meet requirements of USG, state and federal mandates	Aggregation	466 : 26	R
7.02	[President]	[have] ultimate responsibility	for UGA Security Plan, policies, standards, and best practice	that meet requirements of USG, state and federal mandates	Aggregation	466 : 26	R
7.02	[President]	interpret	UGA Policies	[at all times]	Aggregation	466 : 28	R
7.02	audit office	enforce	compliance with UGA security policy	[at all times]	Choice	472 : 29	R

Appendix N "Conduct Analysis"

ACUPA	*A*	*I*	*B*	*C*	*RULE.TYPE*	*DEONTIC*	*ORG*	*REF*
2.02	CISO	determine	likely path	in consultation with the CIO	Aggregation	P	UGA	471 : 2
2.02	The CISO and CIO	set	the agenda and scope	for policy development upon consultation with stakeholders.	Aggregation	R	UGA	471 : 14
2.10	The CIO	make	final decision	as to scope and agenda for policy development activities.	Aggregation	R	UGA	471 : 15
2.01	The CIO and CISO	participate in development	policy	[at all times]	Boundary	R	UGA	382 : 28
2.01	CIO or CISO	identify	policy owners	for particular areas of concern	Boundary	R	UGA	471 : 1
2.03	The CISO and CIO	select	owners of a process or a system, affected by a perceived policy gap need	as team members	Boundary	R	UGA	471 : 8
2.03	The CISO and CIO	select	managers whose area of authority is affected .	as team members	Boundary	P	UGA	471 : 9
2.03	The Office of Legal Affairs, Office of Internal Audit, Office of Finance, Office of Human Resources, Office of Public Affairs, and others named by the CISO	be	members	of the University Security Committee.	Boundary	R	UGA	471 : 20
2.07	Management	identify	stakeholders	ad hoc	Boundary	P	UGA	471 : 7
2.01	Information Technology Security Advisory Council	Develop	policy	when necessary, in accordance with Guidelines and Procedures for Blocking Network Access."	Choice	R	UGA	381 : 27
2.01	ITSAC	develop		[at all times]	Choice	R	UGA	382 : 26
2.01	Office of Information Security	write	minimum security standards for networked devices	[at all times]	Choice	R	UGA	381 : 23
2.02	The CIO and CISO	produce	the policy plan	collaboratively	Choice	R	UGA	471 : 15.1
2.03	CISO	refine	the path, or strategies, taken to achieve policy change	in consultation with team members	Choice	P	UGA	471 : 3

Appendix N Analysis of Statements by Case for "Conduct Analysis"

ACUPA	*A*	*I*	*B*	*C*	*RULE.TYPE*	*DEONTIC*	*ORG*	*REF*
2.04	Office of Legal Affairs	research	the legal obligations and risks posed to the university	as a liability or compliance issue, most of the time	Choice	R	UGA	471 : 11
2.04	team	gather	data	from subject matter expert(s), peer institutions that have similar policies, organizations like Educause, and other appropriate resources.	Choice	R	UGA	471 : 10
2.06	UGA	employ	the ISO 31000 risk management framework	to analyze the risks, costs, and benefits	Choice	R	UGA	471 : 12
2.08	Departments, units, or service providers	develop	stricter standards	as needed	Choice	P	UGA	382 : 12
2.08	University of Georgia Information Security Committee	make	recommendations	to the Director of University Information Security and the Office of the CIO regarding information security strategy, policy, and the awareness and training program.	Choice	R	UGA	472 : 5
2.09	UGA	decide	to write or revise a new policy	only after examining the alternatives carefully.	Choice	R	UGA	471 : 13
2.10	UGA	develop	policy documents that may replicate the mandated policy	If a policy is required by an external organization	Choice	F	UGA	471 : 16
2.10	the university	establish	policy	that defines responsibility of what needs to be done	Choice	R	UGA	472 : 27
2.01	the University of Georgia Information Security Committee	be	the name	of the committee	Position	R	UGA	472 : 3
2.03	Bursar's Office – Elizabeth Quillian	[be]	a member	of the University of Georgia Information Security Committee	Position	R	UGA	472 : 20
2.03	Extended Campuses - Chris Adcock	[be]	a member	of the University of Georgia Information Security Committee	Position	R	UGA	472 : 17
2.03	Faculty & Research –TBD	[be]	a member	of the University of Georgia Information Security Committee	Position	R	UGA	472 : 16
2.03	Human Resources – Duane Ritter	[be]	a member	of the University of Georgia Information Security Committee	Position	R	UGA	472 : 18

Appendix N Analysis of Statements by Case for "Conduct Analysis"

ACUPA	*A*	*I*	*B*	*C*	*RULE.TYPE*	*DEONTIC*	*ORG*	*REF*
2.03	Internal Audit - Will Laney	[be]	a member	of the University of Georgia Information Security Committee	Position	R	UGA	472 : 19
2.03	ITMF - Chris Adcock	[be]	a member	of the University of Georgia Information Security Committee	Position	R	UGA	472 : 15
2.03	Legal Affairs- Tim Kelly	[be]	a member	of the University of Georgia Information Security Committee	Position	R	UGA	472 : 13
2.03	Policy owners	be	individuals responsible for a business process, system or unit of the organization.	[at all times]	Position	P	UGA	471 : 1.1
2.03	Public Affairs- Mitch Clayton	[be]	a member	of the University of Georgia Information Security Committee	Position	R	UGA	472 : 14
2.03	Team members	be	selected individuals	based on the issues and the areas of the university that are affected.	Position	P	UGA	471 : 4
2.03	the CIO, CISO, Office of Legal Affairs, the internal auditor, business process owners, and stakeholders selected by the CISO or CIO	be	members	of the team	Position	R	UGA	471 : 4
2.07	stakeholders	be	groups that exist within the university organization		Position	P	UGA	471 : 5
2.07	stakeholders	be	individuals with an interest in the policy	if no formal organization responsible for that policy exists	Position	P	UGA	471 : 6
2.02	Departments, units, or service providers	develop	stricter standards	for themselves with or without the advice or assistance of the CIO and CISO.	Scope	P	UGA	381 : 11
2.01	[an IT director]	be	Officer(s) of Coordinating Responsibility (OCR)	most of the time	Boundary	R	Ga Southern	336 : 9
2.01	[CIO	be	Officer(s) of Primary Responsibility (OPR)	most of the time	Boundary	R	Ga Southern	336 : 8
2.03	CIO	invite	individuals	to become members of TASC	Boundary	R	Ga Southern	474 : 6

Appendix N Analysis of Statements by Case for "Conduct Analysis"

ACUPA	*A*	*I*	*B*	*C*	*RULE.TYPE*	*DEONTIC*	*ORG*	*REF*
2.03	Officer of Primary Responsibility	involve	Office of Legal Affairs and Internal Audit	Once the Statement of Policy Need is created, as necessary	Boundary	R	Ga Southern	336 : 16
2.03	Officer of Primary Responsibility	involve	subject-matter experts (SME's)	Once the Statement of Policy Need is created, as necessary	Boundary	R	Ga Southern	336 : 13
2.07	Policy Owners	engage	stakeholders committed to sound policy development.	[at all times]	Boundary	R	Ga Southern	473 : 5
2.07	IT Directors	determine	who is or should be affected by policy issue	[at all times]	Boundary	R	Ga Southern	336 : 4
2.02	IT Directors	define	scope of the issue	[at all times]	Choice	R	Ga Southern	336 : 5
2.02	Team	manage	the process	as the team decides	Choice	R	Ga Southern	473 : 10
2.04	Officer of Primary Responsibility	gather	necessary information on the issue(s)	Once the Statement of Policy Need is created,	Choice	R	Ga Southern	336 : 12
2.06	CISO, Legal Affairs, and office of internal audit	perform	risk assessment	on proposed policies and policy changes	Choice	R	Ga Southern	474 : 9
2.09	IT Directors	determine	existence of policy	if policy exists	Choice	R	Ga Southern	336 : 6
2.09	Officer of Primary Responsibility	review	analogous policy(s)	Once the Statement of Policy Need is created, from peer institutions and/or best practices	Choice	R	Ga Southern	336 : 15
2.09	Officer of Primary Responsibility	review	related (pre-existing Georgia Southern) policies	Once the Statement of Policy Need is created,	Choice	R	Ga Southern	336 : 14
2.10	Officer of Primary Responsibility	draft	Policy Concept Document	[once all the actions are completed]	Choice	R	Ga Southern	336 : 17

Appendix N Analysis of Statements by Case for "Conduct Analysis"

ACUPA	*A*	*I*	*B*	*C*	*RULE.TYPE*	*DEONTIC*	*ORG*	*REF*
2.10	IT Directors	deliver	Memoranda	regarding Statement of Policy Need	Information	R	Ga Southern	336 : 10
2.02	Team and stakeholders	receive	commendation	for maintaining pace of development	Payoff	R	Ga Southern	473 : 8
2.01	[an IT director]	be	Officer(s) of Coordinating Responsibility (OCR)	most of the time	Position	R	Ga Southern	336 : 9
2.01	[CIO	be	Officer(s) of Primary Responsibility (OPR)	most of the time	Position	R	Ga Southern	336 : 8
2.07	Stakeholders	include [be]	technical, management, and operational actors.	[at all times]	Position	R	Ga Southern	473 : 4
2.10	each University System of Georgia institution	develop	policy	authorized by BOR Appropriate Use Policy (2009-14) that, at minimum, includes the Board policy guidelines.	Scope	R	Ga Southern	332 : 3
2.04	ISO	works	this material [standards, procedures and guidelines necessary to administer access to university information resources]	to develop in conjunction with information resource owners, the university data administrators and functional users	Aggregation	R	GSU	368 : 53
2.10	Office of Legal Affairs	approve	the draft	[at all times]	Aggregation	R	GSU	470 : 6
2.03	The team	include	the Responsible Office.		Boundary	P	GSU	475 : 4
2.02	University	implement	ISMS	incrementally and scaled in accordance with University requirements	Choice	R	GSU	367 : 3
2.03	CISO	select	team	to determine need for policy.	Choice	R	GSU	470 : 5
2.03	Policy owner	include	all relevant parties	in discussions and formulations.	Choice	P	GSU	475 : 2

Appendix N Analysis of Statements by Case for "Conduct Analysis"

ACUPA	*A*	*I*	*B*	*C*	*RULE.TYPE*	*DEONTIC*	*ORG*	*REF*
2.06	information security personnel	conduct	risk assessments	Where appropriate, of technologies/processes that are being evaluated and/or used at Georgia State University	Choice	R	GSU	371 : 1
2.06	CISO and team	determine	costs	of implementing new policy	Choice	R	GSU	470 : 14
2.08	information security personnel	recommend	security controls	which, if any, are commensurate with the risks to which the university would be exposed.	Choice	P	GSU	371 : 3
2.09	Office of Legal Affairs	approve	the new policy	if umbrella policies cover the need.	Choice	F	GSU	470 : 7
2.09	[University]	develop and enact	an interim policy (and or procedures)	Where legal or compliance imperatives demand an immediate modification (or suspension) of policy (and practice), pending formal review and approval.	Choice	R	GSU	367 : 6
2.10	Organizations that are within the scope of the University's ISMS	establish	safeguards against security threats	[at all times]	Choice	R	GSU	367 : 29
2.01	The administrative office charged with implementing and overseeing the policy	be	the Responsible Office.	[at all times]	Position	R	GSU	475 : 3
2.01	The Information Security Officer (ISO), as designated by the Associate Provost for Information Systems and Technology,	develop	university information security policies	[at all times]	Position	R	GSU	368 : 50
2.01	IS Policy and Compliance Manager (PCM)	kick off	process	when the IS Policy and Compliance Manager (PCM) receives the request to review a policy or write a new policy	Aggregation	R	GT	360 : 22
2.03	GT Internal Audit	comprise	PRC	[at all times]	Boundary	R	GT	360 : 10
2.03	GT Legal	comprise	PRC	[at all times]	Boundary	R	GT	360 : 9

Appendix N Analysis of Statements by Case for "Conduct Analysis"

ACUPA	*A*	*I*	*B*	*C*	*RULE.TYPE*	*DEONTIC*	*ORG*	*REF*
2.03	GT Registrar	comprise	PRC	[at all times]	Boundary	R	GT	360 : 11
2.03	members from GT Legal, HR, OIT, Internal Audit, and Registrar	comprise	PRC		Boundary	R	GT	360 : 5
2.03	OIT-ED	comprise	PRC	[at all times]	Boundary	R	GT	360 : 7
2.03	OIT-EIS	comprise	PRC	[at all times]	Boundary	R	GT	360 : 8
2.03	OIT-IS	comprise	PRC	[at all times]	Boundary	R	GT	360 : 6
2.03	Technology/Service SME	comprise	PRC	[at all times] based on policy/standard	Boundary	R	GT	360 : 12
2.01	Georgia Tech's OIT Information Security (OIT-IS) group	develop	this policy	[at all times]	Choice	R	GT	353 : 24
2.02	OIT-IS	follow	this process, known as Security Policy Review	when writing/revising security policies which will affect OIT and/or Georgia Tech as a whole.	Choice	R	GT	360 : 2
2.08	PCM	document	changes	proposed (if a review) or proposed language (if a new request)	Choice	R	GT	360 : 24
2.08	PCM	perform	analysis	initial of the request	Choice	R	GT	360 : 23
2.00	PRC	provide	feedback and constructive criticism	for proposed OIT and GT Security Policies based on their respective functional areas.	Information	R	GT	360 : 13
2.01	IS Policy and Compliance Manager (PCM)	kick off	policy process	when the IS Policy and Compliance Manager (PCM) receives the request to review a policy or write a new policy.	Information	S	GT	360 : 21
2.07	PCM	seek	input	from the various technical communities on campus (GTITC, CSS, CSR's, while writing the new policy or updating existing policies	Information	R	GT	360 : 27
2.09	PCM	forward	information	to the OIT IS Director for preliminary approval to proceed.	Information	R	GT	360 : 25

Appendix N Analysis of Statements by Case for "Conduct Analysis"

ACUPA	*A*	*I*	*B*	*C*	*RULE.TYPE*	*DEONTIC*	*ORG*	*REF*
2.10	[GT organizations]	reduce	minimum requirements established in this policy	[in] Other policies, standards, procedures, and safeguards documents	Scope	F	GT	344 : 14
2.10	[GT organizations]	augment	restrictions	for the sake of security [in] Other policies, standards, procedures, and safeguards documents	Scope	P	GT	343 : 13
2.10	[GT]	submit	policy	to applicable federal and State statutes and regulations that guarantee either protection or accessibility of Institute records]	Scope	R	GT	344 : 5
2.10	[GT]	submit	policy	to applicable federal and State statutes and regulations that guarantee either protection or accessibility of Institute records [will take precedence over this policy]	Scope	R	GT	344 : 5

Appendix O "Draft Policy"

ACUPA	A	I	B	C	RULE.TYPE	DEONTIC	ORGANIZATION	REF
3.01	ITSAC and OIS	responsible		for the accuracy of the subject matter	Aggregation	R	UGA	381 : 35
3.04	The Information Technology Management Forum (ITMF) Security Committee	provide	input	on "standards and policy development … involving the campus as a whole" .	Choice	R	UGA	472 : 22
3.04	The University Security Committee	make	policy recommendations	to the CIO and CISO	Choice	R	UGA	471 : 18
3.03	the CISO	socialize	the policy/issue and plan	with most of the affected parties during the drafting to help gain support for the policy change	Information	R	UGA	472 : 21
3.01	CIO	determine	the period (time and frequency)	for students, employees, and service providers to re-affirm their recognition of this policy.	Aggregation	R	Ga Southern	332 : 23.2
3.02	OPR	determine	who will be responsible for drafting the policy and procedures	once input on the concept document has been obtained	Aggregation	R	Ga Southern	336 : 27.1
3.02	OPR	determine	who will be responsible for drafting the policy and procedures	once input on the concept document has been obtained	Boundary	R	Ga Southern	336 : 27.1
3.01	Team	simplify	policy	to minimize effort required to comply.	Choice	R	Ga Southern	473 : 9
3.02	OCR	develop	initial draft policy and accompanying procedures	once input on the concept document has been obtained,utilizing the IT Policy templates to ensure consistency	Choice	R	Ga Southern	336 : 28
3.02	Officer(s) of Coordinating Responsibility (OCR)	write	draft of the policy and operational procedures	Once input on the concept document has been obtained	Choice	P	Ga Southern	336 : 24
3.04	Information Technology Advisory Council	provide	feedback	on issues regarding instructional technologies	Choice	R	Ga Southern	474 : 8
3.03	Officer(s) of Primary Responsibility (OPR) / Officer(s) of Coordinating Responsibility (OCR)	inform	stakeholders	[when distributing policy concept document] of possible changes to policies	Information	R	Ga Southern	336 : 21
3.03	Officer(s) of Primary Responsibility (OPR) /	solicit	input	from all stakeholders [regarding draft policy concept document]	Information	R	Ga Southern	336 : 20

Appendix O "Draft Policy"

	Officer(s) of Coordinating Responsibility (OCR)							
3.03	Officer(s) of Primary Responsibility (OPR) / Officer(s) of Coordinating Responsibility (OCR)	distribute	policy concept document	to all stakeholders	Information	R	Ga Southern	336 : 19
3.03	Officer(s) of Primary Responsibility (OPR) / Officer(s) of Coordinating Responsibility (OCR)	inform	stakeholders	[when distributing policy concept document] how it affects them	Information	R	Ga Southern	336 : 22
3.03	Team	exchange	information	in face-to-face meetings as much as possible	Information	R	Ga Southern	473 : 6
3.05	Team	receive	commendation	for maintaining progress by delivery of working policies	Payoff	R	Ga Southern	473 : 7
3.02	CISO	draft	draft policy	using approved format	Choice	R	GSU	470 : 13
3.02	Team	draft	policy	to present to key stakeholders	Choice	R	GSU	470 : 4
3.02	Team	use	the Policy Template	for all new policies and policy revisions	Choice	R	GSU	475 : 5
3.02	Office of Internal Audits	draft	policy	[at all times]	Choice	F	GSU	470 : 3
3.03	Team	revise	draft policy	accomodating comments by Office of Legal affairs	Choice	R	GSU	470 : 8
3.04	CIO	present	draft policy	to ISAT for examination and discussion if Legal approves and CIO approves	Choice	R	GSU	470 : 11
3.03	CISO	present	draft	to Internal Audits for comments	Information	R	GSU	470 : 9
3.03	CISO	present	draft policy	to CIO	Information	R	GSU	470 : 10
3.02	PCM	write	initial draft	Once approval from the OIT IS Director has been received, taking into account the edits from the OIT IS Director.	Choice	R	GT	360 : 26
3.05	PRC	review	proposed changes	over a period not to exceed 1 month.	Choice	R	GT	360 : 31

Appendix O "Draft Policy"

3.02	PCM	include	summary of proposed changes or new policy highlights	with the draft.	Information	R	GT	360 : 29
3.03	PCM	socialize	draft	with various groups (e.g. SGA, Faculty and Technical Leads) for feedback where appropriate	Information	R	GT	360 : 30
3.03	PCM	send	initial draft	to the PRC for review.	Information	R	GT	360 : 28
3.04	CIO	vet	proposal	with executive leadership team	Information	P	GT	476 : 1
3.04	Information Security Office	vet	policy proposal	with HR, Legal Affairs prior to vetting with campus units	Information	R	GT	476 : 11
3.04	Information Security Office	vet	proposal	with faculty excutive board, faculty senate, and all units of the campus	Information	R	GT	476 : 2
3.04	Information Security Office	solicit	information	from campus units after proposal/need vetted with executive leadership	Information	R	GT	476 : 4
3.04	Information Security Office	meet	associate dean and IT director for a campus unit	to discuss changes	Information	R	GT	476 : 6
3.05	PRC	handle	initial discussion	During this time, over email with weekly face-face meetings as needed.	Information	R	GT	360 : 32
3.05	PRC Members	are	input	expected to provide input based on their functional areas.	Information	S	GT	360 : 33

Appendix P "Get Approvals"

ACUPA	A	I	B	C	RULE TYPE	DEONTIC	ORG	REF
4.02	Office of Information Security	approve	exceptions to minimum security standards	[at all times]	Aggregation	R	UGA	381 : 24
4.04	ITSAC and the Offices of the CIO and CISO	approve changes to the UGA Password Standard		[at all times]	Aggregation	R	UGA	382 : 37
4.04	Office of the CIO and the Chief Information Security Officer	final arbitration		for policy exception review	Aggregation	R	UGA	381 : 29
4.04	CIO	approve	draft policy	[at all times]	Aggregation	R	UGA	472 : 24
4.04	the President	approve	draft policy	[at all times]	Aggregation	R	UGA	472 : 25
4.04	the president's cabinet	approve	draft policy	[at all times]	Aggregation	R	UGA	472 : 23
4.04	Departments, units, and individuals	request from the Chief Information Security Officer (CISO)	exemption	if unable to comply with the UGA Password Standard	Choice	R	UGA	382 : 13
4.04	The UGA Office of Information Security	process through the Information Technology Security Advisory Council	the request for final approval	[at all times]	Choice	R	UGA	382 : 14
4.03	Officer(s) of Primary Responsibility (OPR) / Officer(s) of Coordinating Responsibility (OCR)	make	revisions	as necessary, to draft policy	Choice	R	Ga Southern	336 : 33
4.03	Policy Owner	revise	documents	documents upon feedback from advisory committees within 24-48 hours of feedback.	Choice	R	Ga Southern	474 : 7
4.01	Officer(s) of Primary Responsibility (OPR) / Officer(s) of	present	draft policy	typically 30 days for consideration by President's Cabinet and relevant audiences	Information	R	Ga Southern	336 : 31

Appendix P "Get Approvals"

ACUPA	A	I	B	C	RULE TYPE	DEONTIC	ORG	REF
	Coordinating Responsibility (OCR)							
4.01	Officer(s) of Primary Responsibility (OPR) / Officer(s) of Coordinating Responsibility (OCR)	present	draft policy	typically 30 days for consideration by President's Cabinet and relevant audiences	Information	R	Ga Southern	336 : 31
4.03	Policy Owners	accept	stakeholder input	anytime in the cycle	Information	R	Ga Southern	473 : 2
4.03	Officer(s) of Primary Responsibility (OPR) / Officer(s) of Coordinating Responsibility (OCR)	address	requests	for additional information, clarifications, objections, recommendations, etc.	Information	R	Ga Southern	336 : 32
4.03	Team	deliver	viable policy drafts	frequently during the development process.	Information	R	Ga Southern	473 : 3
4.04	OPR (CIO)	seek	policy approval	from President's Cabinet by submitting amended draft with date and version accordingly	Information	R	Ga Southern	336 : 35
4.03	Policy Owners	satisfy	the stakeholders	through timely and continuous policy actions	Scope	R	Ga Southern	473 : 1
4.02	The Senate	pass or deny	the motion to approve	[at all times]	Aggregation	R	GSU	475 : 20
4.04	The Administrative Council	recommend	approval or denial	to the President	Aggregation	R	GSU	475 : 31
4.04	The President	deny or approve	the proposed policy.	when presented proposal by Administrative Council	Aggregation	R	GSU	475 : 32
4.04	The President	concur or veto	the motion of the Senate	[at all times]	Aggregation	R	GSU	475 : 21
4.04	the University Senate (academic and Student Policies) or the Administrative Council (administrative policies)	approve	All university-wide policies	prior to final approval by the President, as set forth in University Statutes.	Aggregation	R	GSU	475 : 13
4.01	The provost	appoint	members	of the Policy Advisory Group	Boundary	R	GSU	475 : 10

Appendix P "Get Approvals"

ACUPA	A	I	B	C	RULE TYPE	DEONTIC	ORG	REF
4.01	the Office of Institutional Effectiveness	arrange	the policy draft	to be reviewed by the Policy Advisory Group.	Choice	R	GSU	475 : 7
4.01	The Policy Advisory Group (PAG)	review	drafts of policies	to ensure that all mandatory elements are completed, that format is consistent, and that any overlaps with policies or conflicts with other policies or federal, state, or Board of Regents regulations are identified prior to its final approval.	Choice	R	GSU	475 : 8
4.01	The Policy Advisory Group (PAG)	evaluate	proposed policy	(at all times)	Choice	F	GSU	475 : 9
4.02	Administrative Council	approve	new policies or revisions to existing policies	if administrative or operational policies	Choice	R	GSU	475 : 11
4.02	The Administrative Council	discuss	the proposed policy	if introduced to the council	Choice	R	GSU	475 : 30
4.02	The Policy Advisory Group	review	drafts of new or revised policy	to (a) ensure that all mandatory elements are completed and consistency of format, and (b) identify any overlap with other policies or conflict with other policies or federal, state, and Board of Regents regulations.	Choice	R	GSU	475 : 26
4.02	The Policy Advisory Group	complete	reviews	in a maximum of 5 working days (urgent issues will be expedited).	Choice	R	GSU	475 : 16
4.02	The Policy Advisory Group	complete	reviews	in a maximum of 5 working days (urgent issues will be expedited).	Choice	R	GSU	475 : 27
4.02	The Policy Advisory Group	review	drafts of new or revised policy	to (a) ensure that all mandatory elements are completed and consistency of format, and (b) identify any overlap with other policies or conflict with other policies or federal, state, and Board of Regents regulations.	Choice	R	GSU	475 : 15
4.02	The Senate	discuss	the policy	when introduced	Choice	R	GSU	475 : 19
4.02	University Senate	approve	new policies or revisions to existing policies	if policy is academic or student related	Choice	R	GSU	475 : 11

Appendix P "Get Approvals"

ACUPA	A	I	B	C	RULE TYPE	DEONTIC	ORG	REF
4.03	The Policy Advisory Group	return	the draft policy documents	to the Responsible Executive (e.g. vice president, associate provost) for introduction to the Administrative Council.	Choice	R	GSU	475 : 28
4.03	the Responsible Office	draft	the new policy or revision of existing policy.	With input from any interested parties and the relevant vice president or associate provost,	Choice	R	GSU	475 : 25
4.03	the Responsible Office and/or the relevant Senate Committee	draft	document containing the new policy or revises an existing policy.	With input from the relevant associate provost or vice president,	Choice	R	GSU	475 : 14
4.01	CIO	present	draft policy	to Admin Council	Information	R	GSU	470 : 12
4.01	[Team]	submit	policy drafts	to the Office of Institutional Effectiveness	Information	R	GSU	475 : 6
4.03	The Policy Advisory Group	return	draft policy document	to the Responsible Office/Senate Committee for scheduling the discussion of the policy on the University Senate Agenda.	Information	R	GSU	475 : 17
4.02	the chair of that committee	be	sponsor of the proposed policy	when the policy is introduced in the Senate, If the drafted policy comes under the purview of the Senate Committee	Position	R	GSU	475 : 18
4.02	The Office of Institutional Effectiveness	be	[responsible office]	for overseeing the policy management process	Position	R	GSU	475 : 12
4.02	the relevant associate provost or vice president	be	sponsor of the proposed policy	if not [under the purview of the Senate]	Position	R	GSU	475 : 19
4.02	The Responsible Executive	[be]	sponsor	of the proposed policy when the policy is introduced in the Administrative Council.	Position	R	GSU	475 : 29
4.04	President of the Georgia Institute of Technology	[provide]	final approval of this policy	based on a review by the Information Security Policy Committee	Aggregation	R	GT	348 : 8
4.02	PRC	review	new policies, which will be written by OIT-IS	prior to CIO approval and policy publication	Choice	R	GT	360 : 15

Appendix P "Get Approvals"

ACUPA	A	I	B	C	RULE TYPE	DEONTIC	ORG	REF
4.02	PRC Members	compile	final draft	At the end of 1 month, taking into account the various inputs and recommendations.	Choice	R	GT	360 : 34
4.01	PCM	keep apprised (or apprise)	PRC	of the discussions with the CIO and any changes that are proposed	Information	R	GT	360 : 37
4.03	Information Security Office	present	final draft	to Faculty Executive Board prior to seeking approval.	Information	R	GT	476 : 8
4.03	Information Security Office	meet	faculty senate committee	to review draft	Information	R	GT	476 : 7
4.03	PCM	pass	approved PRC draft	to the CIO for approval.	Information	R	GT	360 : 35
4.03	PCM	brief	CIO	on the proposed changes or new policy	Information	R	GT	360 : 36
4.03	PCM	take	recommendations the CIO has	into account	Information	R	GT	360 : 36.1
4.02	PRC	review	changes	Grammatical, format, or minor (e.g. contact information)	Scope	F	GT	360 : 16

Appendix Q "Education (Awareness)"

ACUPA	A	I	B	C	RULE TYPE	DEONTIC	ORG	REF
5.01	Policy Owners	develop	awareness activities	to inform stakeholders who will place the requirements into practice.	Choice	R	UGA	471 : 17
5.04	The Office of Information Security	provide	training	[at all times]	Choice	R	UGA	382 : 22
5.01	CISO	develop	awareness and training program	(at all times)	Choice	R	Ga Southern	474 : 10
5.01	OCR	Develop	a communication plan / matrix	once input on the concept document has been obtained,for introducing the new policy	Choice	R	Ga Southern	336 : 29
5.02	Officer(s) of Coordinating Responsibility (OCR)	post	the policy and procedures	to VPIT policy website Once approved,	Information	R	Ga Southern	336 : 37
5.03	Officer(s) of Coordinating Responsibility (OCR)	post	approved policy	in master repository ensuring proper classification for easy reference	Information	R	Ga Southern	336 : 40
5.04	Officer(s) of Coordinating Responsibility (OCR)	distribute	policy document	as per communication plan	Information	R	Ga Southern	336 : 41
5.04	Officer(s) of Coordinating Responsibility (OCR)	distribute	the policy and procedures	Once approved, according to the established communication plan	Information	R	Ga Southern	336 : 39
5.04	Officer(s) of Coordinating Responsibility (OCR)	distribute	the policy and procedures	Once approved, according to the established communication plan	Information	R	Ga Southern	336 : 39
5.02	The Associate Provost	post	the approved policy	on the University's policy website.	Choice	R	GSU	475 : 23
5.02	[University]	make available	applicable documents	at points of use relevant versions	Information	R	GSU	367 : 9
5.02	The Associate Provost	post	the approved policy.	on the University Website	Information	R	GSU	475 : 33
5.04	[Information Security Department]	make aware	All relevant personnel	of the relevance and importance of their information security activities and how they contribute to the achievement of the ISMS objectives	Information	R	GSU	367 : 27

Appendix Q "Education (Awareness)"

ACUPA	A	I	B	C	RULE TYPE	DEONTIC	ORG	REF
5.04	The Responsible Office or Senate Committee	notify	relevant individuals and departments	of the policy change.	Information	R	GSU	475 : 24
5.04	The Responsible Ofice	notify	relevant individuals and departments	of the policy change	Information	R	GSU	475 : 34
5.01	The responsible university officer	notify via email and/or in writing	associate vice provosts; deans, associate vice presidents, unit heads, internal auditing, office of legal affairs, OIT information security, technical leads	upon approval of the policy and upon any subsequent revisions or amendments made to the original document	Information	R	GT	343 : 187
5.02	[Institute]	publish	this policy	upon approval on the Georgia Tech website	Information	O	GT	344 : 71
5.02	PCM	update and post	final draft	to the OIT Policy Website, once the CIO has approved the final draft	Information	R	GT	360 : 39
5.02	PCM	communicate	final document	via email to the campus, once the draft or changes have been approved	Information	R	GT	360 : 38
5.02	The responsible university officer	publish on the Georgia Tech website	this policy	upon approval	Information	R	GT	343 : 186
5.04	Georgia Tech Academic and Administrative units, including OIT,	communicate	this policy	to their users	Information	R	GT	353 : 26
5.04	OIT-IS	publish	this policy	upon approval	Information	R	GT	353 : 29
5.04	OIT-IS	notify	CIO	of the changes [grammatical, format, or minor] and publish them as necessary.	Information	R	GT	360 : 17

Appendix R "Plan Maintenance"

ACUPA	A	I	B	C	RULE TYPE	DEONTIC	ORG	REF
6.04	The CIO and CISO	serve as the final arbitrators		in policy exception review	Aggregation	R	UGA	382 : 30
6.04	The CIO and CISO	serve as the final arbitrators		in policy exception review	Aggregation	R	UGA	382 : 30
6.04	ITSAC	participate in policy exception review		[at all times]	Boundary	R	UGA	382 : 27
6.04	The Office of Information Security	participate in policy exceptions review		[at all times]	Boundary	R	UGA	382 : 25
6.03	ITSAC and OIS	review	policy	on an annual basis	Choice	R	UGA	381 : 34
6.03	[UGA}	update	this policy	as needed as card association regulations change	Choice	R	UGA	380 : 3
6.03	CISO, in cooperation with the ITMF-SECCOMM	review	the policy and standards	on an annual basis	Choice	R	UGA	378 : 45
6.03	CISO, in cooperation with the ITSAC	review	policy and standards	on an annual basis	Choice	R	UGA	382 : 35
6.03	CISO, in cooperation with the ITSAC	review	policy and standards	on an annual basis	Choice	R	UGA	382 : 35
6.03	The Office of Information Security	develop and review	this policy	on a regular basis	Choice	R	UGA	382 : 24
6.03	The Office of the Chief Information Officer, in cooperation with the University Security Committee	review	this policy	on an annual basis	Choice	O	UGA	376 : 32

Appendix R "Plan Maintenance"

ACUPA	A	I	B	C	RULE TYPE	DEONTIC	ORG	REF
6.04	Office of Information Security	develop and review	university-wide information security policy and procedures	[at all times]	Choice	R	UGA	381 : 22
6.04	The CIO and CISO	review	policy	[at all times]	Choice	R	UGA	382 : 29
6.04	[President]	review	development, execution and maintenance of UGA Security Plan	in concert with requirements of USG, state and federal mandates	Choice	R	UGA	466 : 27
6.04	The University Security Committee	review	policy	as needed	Choice	R	UGA	471 : 19
6.05	University of Georgia Information Security Committee	[provide]	Recommendation	for improvement of Role-Based Accountability model and the University's information security training and awareness program	Choice	R	UGA	472 : 11
6.05	University of Georgia Information Security Committee	[provide]	Feedback and guidance	on development of a comprehensive IT Security Strategy encompassing people, processes and technology	Choice	R	UGA	472 : 9
6.05	University of Georgia Information Security Committee	provide	critical analysis and feedback	on existing or proposed policies and initiatives related to information security and privacy to the Director of University Information Security and the Office of the CIO.	Choice	R	UGA	472 : 7
6.07	Officer(s) of Coordinating Responsibility (OCR)	[determine]	new policy	due to extensive changes necessary? Is a new policy required	Aggregation	R	Ga Southern	336 : 48
6.07	Officer(s) of Coordinating Responsibility (OCR)	determine		if policy ist still needed/applicable	Aggregation	R	Ga Southern	336 : 46
6.01	Officer(s) of Coordinating Responsibility (OCR)	date and version	[amended policy]	[at all times]	Choice	R	Ga Southern	336 : 50
6.02	Officer(s) of Coordinating Responsibility (OCR)	create	a master backup	Once approved,	Choice	R	Ga Southern	336 : 38
6.02	Officer(s) of Coordinating Responsibility (OCR)	Move	Retired/obsolete policy document	to a Policy Archive, ensuring correct classification to enable future reference	Choice	R	Ga Southern	336 : 53

Appendix R "Plan Maintenance"

ACUPA	A	I	B	C	RULE TYPE	DEONTIC	ORG	REF
6.03	Officer(s) of Coordinating Responsibility (OCR)	review	the policy	periodically	Choice	R	Ga Southern	336 : 44
6.04	CISO and Procurement	collaborate		in some instances to review policy	Choice	R	Ga Southern	474 : 3
6.04	Officer(s) of Coordinating Responsibility (OCR)	oversee	policy implementation	[at all times]	Choice	R	Ga Southern	336 : 42
6.04	TASC (Advisory committee)	review	policy changes	(at all times)	Choice	R	Ga Southern	474 : 5
6.04	Team	review	the Policy Process	for effectiveness on a regular basis	Choice	R	Ga Southern	473 : 11
6.06	CISO and Internal Audit Office	collaborate		to review risk	Choice	R	Ga Southern	474 : 1
6.06	CISO and legal affairs office	collaborate		to review risk	Choice	R	Ga Southern	474 : 2
6.06	Office of legal affairs	vet	policies	from a legal risk management perspective most of the time	Choice	R	Ga Southern	474 : 4
6.06	Officer(s) of Coordinating Responsibility (OCR)	evaluate	policy	as per the review schedule specified in the policy itself	Choice	R	Ga Southern	336 : 45
6.07	Officer(s) of Coordinating Responsibility (OCR)	amend, update, modify	[policy]	as necessary	Choice	R	Ga Southern	336 : 47
6.07	Officer(s) of Coordinating Responsibility (OCR)	obtain	approval for changes	as required	Choice	R	Ga Southern	336 : 49
6.02	Officer(s) of Coordinating Responsibility (OCR)	Communicate	policy retirement	as per Communication Plan	Information	R	Ga Southern	336 : 54
6.07	Information Technology Senate Sub-Committee (ITSS)	change	This document and any of the catalogued policies	with such changes being reviewed and recommended through the Senate Information Systems and Technology Committee (ISAT)	Aggregation	P	GSU	361 : 20
6.04	information security personnel	perform	security reviews	In these situations; to determine the threats, the likelihood of such events taking place, the estimated impact if	Choice	S	GSU	371 : 6

Appendix R "Plan Maintenance"

ACUPA	A	I	B	C	RULE TYPE	DEONTIC	ORG	REF
				they were to occur and recommend controls.				
6.04	information security personnel	perform	security reviews	In these situations; to determine the threats, the likelihood of such events taking place, the estimated impact if they were to occur and recommend controls.	Choice	S	GSU	371 : 6
6.07	Organizations that are within the scope of the University's ISMS	ensure	appropriateness of safeguards against security threats	[at all times]	Choice	R	GSU	367 : 29.2
6.01	[Information Security Department]	include	Point(s) of contact for questions or comments	When a new procedure, or version of a procedure, is issued for inclusion in the University's Information Security Management System	Information	R	GSU	367 : 11
6.01	[Information Security Department]	include	Date of last update or issuance	When a new procedure, or version of a procedure, is issued for inclusion in the University's Information Security Management System	Information	R	GSU	367 : 12
6.01	[Information Security Department]	include	Data classification (if sensitive or confidential)	When a new procedure, or version of a procedure, is issued for inclusion in the University's Information Security Management System	Information	R	GSU	367 : 13
6.01	[Information Security Department]	include	A revision level showing the new document(s)/version(s)	When a new procedure, or version of a procedure, is issued for inclusion in the University's Information Security Management System	Information	R	GSU	367 : 10
6.03	[Information Security Department]	hold	meetings	for management reviews semiannually	Information	R	GSU	367 : 18
6.04	[Information Security Department]	include	Follow-up actions from previous management reviews	in the management reviews	Information	R	GSU	367 : 25
6.04	[Information Security Department]	include	Results from effectiveness measurements	in the management reviews	Information	R	GSU	367 : 24

Appendix R "Plan Maintenance"

ACUPA	A	I	B	C	RULE TYPE	DEONTIC	ORG	REF
6.04	[Information Security Department]	include	Vulnerabilities or threats not adequately addressed in the previous risk assessments	in the management reviews	Information	R	GSU	367 : 23
6.04	[Information Security Department]	include	Status of preventive and corrective actions	in the management reviews	Information	R	GSU	367 : 22
6.04	[Information Security Department]	include	Techniques, products or procedures, which could be used at the University to improve the ISMS's performance and effectiveness	in the management reviews	Information	R	GSU	367 : 21
6.04	[Information Security Department]	include	Results of ISMS audits and reviews	in the management reviews	Information	R	GSU	367 : 19
6.04	[Information Security Department]	include	Feedback from interested parties	in the management reviews	Information	R	GSU	367 : 20
6.04	the Georgia Tech Associate Vice President and Associate Vice-Provost for Information Technology.	change	The Computer & Network Security Policy and Procedures	by directive	Aggregation	P	GT	343 : 184
6.04	The responsible university officer	change	this policy	[at all times]	Aggregation	P	GT	343 : 183
6.07	Only he President of the Georgia Institute of Technology.	revise	this policy	by signature	Aggregation	P	GT	348 : 78
6.05	OIT-IS, Internal Audit, and the Unit	involve	qualified information security professionals	in the exception review process	Boundary	R	GT	353 : 14
6.01	Georgia Tech's OIT Information Security (OIT-IS) group	maintain	this policy	[at all times]	Choice	R	GT	353 : 25

Appendix R "Plan Maintenance"

ACUPA	A	I	B	C	RULE TYPE	DEONTIC	ORG	REF
6.01	Georgia Tech's OIT Information Security (OIT-IS) group	maintain	this policy	[at all times]	Choice	R	GT	353 : 25
6.03	OIT-IS, Internal Audit, and the Unit	review	approved exceptions	periodically	Choice	R	GT	353 : 16
6.03	PRC	review	Security Policies/Standards/Procedures	on an annual basis, based on the initial publication date.	Choice	R	GT	360 : 14
6.04	OIT-IS, Internal Audit, and the Unit	review	Any deviation from security policies and standards	ia the Information Security Exception Review Process	Choice	R	GT	353 : 13
6.05	OIT-IS, Internal Audit, and the Unit	require	the Unit Head, CIO, EVP, or Provost.	to approve exemption requests involving potentially significant risk to the Unit	Choice	P	GT	353 : 17
6.05	OIT-IS, Internal Audit, and the Unit	log	all findings and results	in a central repository that is accessible to all Georgia Tech staff involved in the assessement of the exception request.	Choice	R	GT	353 : 15
6.06	business processs	take precedenc e over	these policies [security policies and standards]	when there will be times	Choice	S	GT	353 : 5
6.06	Information Security Office	do	internal risk assessments	annually	Choice	R	GT	476 : 9
6.06	Information Security Office	contract	external risk assessments	every three years	Choice	R	GT	476 : 10
6.06	OIT-IS, Internal Audit, and the Unit	approve	exception requests	that create significant risks without compensating controls	Choice	F	GT	353 : 20
6.06	OIT-IS, Internal Audit, and the Unit	take into account	what value the exception will bring	to the Unit requesting the exception	Choice	R	GT	353 : 19
6.06	OIT-IS, Internal Audit, and the Unit	evaluate	exception requests	consistently in accordance with Georgia Tech's risk acceptance practice	Choice	R	GT	353 : 21
6.06	Unit	consider	what risks they may face by not adhering to the policy as well as the benefit gained by requesting the exception.	before doing so [requesting an exception]	Choice	S	GT	359 : 2
6.06	we	consider	the security of Georgia Tech's infrastructure and data.	still	Choice	R	GT	353 : 6
6.07	OIT-IS, Internal Audit, and the Unit	evaluate	exception requests	in the context of potential risk to the Unit and Georgia Tech as a whole	Choice	R	GT	353 : 18
6.04	Georgia Tech Academic and	submit	risk exception requests	via the approved process	Information	R	GT	353 : 27

Appendix R "Plan Maintenance"

ACUPA	A	I	B	C	RULE TYPE	DEONTIC	ORG	REF
	Administrative units, including OIT,							
6.05	OIT-IS	notify	the following groups: OIT, Campus Deans and Chairs, Unit Business/Administrative Leads, Georgia Tech IT directors, ITAC, Campus CSR's, Internal Audit	via email and/or in writing upon approval of the standard and upon subsequent reviewsion or amendmnets made to the original document	Information	R	GT	353 : 30
6.05	The responsible university officer	communicate	Any changes to the policy or procedures	promptly to the individuals and offices noted in section 8	Information	R	GT	343 : 185

Appendix S "Measurement and Compliance"

ACUPA	A	I	B	C	RULE TYPE	DEONTIC	ORG	REF
7.02	[President]	[have] ultimate responsibility	for UGA Security Plan, policies, standards, and best practice	that meet requirements of USG, state and federal mandates	Aggregation	R	UGA	466 : 26
7.02	[President]	interpret	UGA Policies	[at all times]	Aggregation	R	UGA	466 : 28
7.02	[President]	[have] ultimate responsibility	for UGA Security Plan, policies, standards, and best practice	that meet requirements of USG, state and federal mandates	Aggregation	R	UGA	466 : 26
7.01	Departments	determine	how to comply with policy	in some cases.	Choice	P	UGA	472 : 28
7.02	audit office	enforce	compliance with UGA security policy	[at all times]	Choice	R	UGA	472 : 29
7.01	ISO	coordinates	standards, procedures and guidelines necessary to administer access to university information resources.	[at all times]	Aggregation	R	GSU	368 : 52
7.01	auditors	possess to enable them to act in accordance with the principles of auditing	personal attributes	[at all times]	Boundary	R	GSU	367 : 16
7.01	[University]	conduct	Internal audits	of the ISMS at planned intervals at least annually	Choice	R	GSU	367 : 14
7.01	[Information Security Department]	maintain	ISMS records	unless specified othewise, in the department or college in which they were produced for a minimum of 30 days.	Choice	R	GSU	367 : 26
7.01	The Information Security Officer (ISO), as designated by the Associate Provost for Information Systems and Technology,	monitor	compliance with those policies and all applicable laws, rules and regulations	[at all times]	Choice	R	GSU	368 : 51
7.00	Campus Units	supersede	institutional policy	with their policy.	Scope	F	GT	476 : 5

Appendix T Aggregation Rules

ACUPA	A	I	B	C	Org	ref	Deontic
2.02	CISO	determine	likely path	in consultation with the CIO	UGA	471 : 2	P
2.02	The CISO and CIO	set	the agenda and scope	for policy development upon consultation with stakeholders.	UGA	471 : 14	R
2.10	The CISO	make	final decision	as to scope and agenda for policy development activities.	UGA	471 : 15	R
3.01	ITSAC and OIS	responsible		for the accuracy of the subject matter	UGA	381 : 35	R
4.02	Office of Information Security	approve	exceptions to minimum security standards	[at all times]	UGA	381 : 24	R
4.04	the presidents cabinet	approve	draft policy	[at all times]	UGA	472 : 23	R
4.04	CIO	approve	draft policy	[at all times]	UGA	472 : 24	R
4.04	the President	approve	draft policy	[at all times]	UGA	472 : 25	R
4.04	Office of the CIO and the Chief Information Security Officer	final arbitration		for policy exception review	UGA	381 : 29	R
4.04	ITSAC and the Offices of the CIO and CISO	approve changes to the UGA Password Standard		[at all times]	UGA	382 : 37	R
6.04	The CIO and CISO	serve as the final arbitrators		in policy exception review	UGA	382 : 30	R
6.04	The CIO and CISO	serve as the final arbitrators		in policy exception review	UGA	382 : 30	R
7.02	[President]	[have] ultimate responsibility	for UGA Security Plan, policies, standards, and best practice	that meet requirements of USG, state and federal mandates	UGA	466 : 26	R
7.02	[President]	[have] ultimate responsibility	for UGA Security Plan, policies, standards, and best practice	that meet requirements of USG, state and federal mandates	UGA	466 : 26	R
7.02	[President]	interpret	UGA Policies	[at all times]	UGA	466 : 28	R
3.01	CIO	determine	the period (time and frequency)	for students, employees, and service providers to re-affirm their recognition of this policy.	Ga Southern	332 : 23.2	R
3.02	OPR	determine	who will be responsible for drafting the policy and procedures	once input on the concept document has been obtained	Ga Southern	336 : 27.1	R

Appendix T Aggregation Rules

ACUPA	A	I	B	C	Org	ref	Deontic
6.07	Officer(s) of Coordinating Responsibility (OCR)	determine		if policy ist still needed/applicable	Ga Southern	336 : 46	R
6.07	Officer(s) of Coordinating Responsibility (OCR)	[determine]	new policy	due to extensive changes necessary? Is a new policy required	Ga Southern	336 : 48	R
2.04	ISO	works	this material [standards, procedures and guidelines necessary to administer access to university information resources]	to develop in conjunction with information resource owners, the university data administrators and functional users	GSU	368 : 53	R
2.10	Office of Legal Affairs	approve	the draft	[at all times]	GSU	470 : 6	R
4.02	The Senate	pass or deny	the motion to approve	[at all times]	GSU	475 : 20	R
4.04	the University Senate (academic and Student Policies) or the Administrative Council (administrative policies)	approve	All university-wide policies	prior to final approval by the President, as set forth in University Statutes.	GSU	475 : 13	R
4.04	The President	concur or veto	the motion of the Senate	[at all times]	GSU	475 : 21	R
4.04	The Administrative Council	recommend	approval or denial	to the President	GSU	475 : 31	R
4.04	The President	deny or approve	the proposed policy.	when presented proposal by Administrative Council	GSU	475 : 32	R
6.07	Information Technology Senate Sub-Committee (ITSS)	change	This document and any of the catalogued policies	with such changes being reviewed and recommended through the Senate Information Systems and Technology Committee (ISAT)	GSU	361 : 20	P
7.01	ISO	coordinates	standards, procedures and guidelines necessary to administer access to university information resources.	[at all times]	GSU	368 : 52	R
2.01	IS Policy and Compliance Manager (PCM)	kick off	process	when the IS Policy and Compliance Manager (PCM) receives the request to review a policy or write a new policy	GT	360 : 22	R

Appendix T Aggregation Rules

ACUPA	A	I	B	C	Org	ref	Deontic
4.04	President of the Georgia Institute of Technology	[provide]	final approval of this policy	based on a review by the Information Security Policy Committee	GT	348 : 8	R
6.04	The responsible university officer	change	this policy	[at all times]	GT	343 : 183	P
6.04	the Georgia Tech Associate Vice President and Associate Vice-Provost for Information Technology.	change	The Computer & Network Security Policy and Procedures	by directive	GT	343 : 184	P
6.07	Only the President of the Georgia Institute of Technology.	revise	this policy	by signature	GT	348 : 78	P

Appendix U Get Approval Rules – Filtered

ACUPA	A	I	B	C	RULE TYPE	DEONTIC	ORG	REF
4.02	Office of Information Security	approve	exceptions to minimum security standards	[at all times]	Aggregation	R	UGA	381 : 24
4.04	ITSAC and the Offices of the CIO and CISO	approve changes to the UGA Password Standard		[at all times]	Aggregation	R	UGA	382 : 37
4.04	Office of the CIO and the Chief Information Security Officer	final arbitration		for policy exception review	Aggregation	R	UGA	381 : 29
4.04	Departments, units, and individuals	request from the Chief Information Security Officer (CISO)	exemption	if unable to comply with the UGA Password Standard	Choice	R	UGA	382 : 13
4.04	The UGA Office of Information Security	process through the Information Technology Security Advisory Council	the request for final approval	[at all times]	Choice	R	UGA	382 : 14
4.03	Officer(s) of Primary Responsibility (OPR) / Officer(s) of Coordinating Responsibility (OCR)	make	revisions	as necessary, to draft policy	Choice	R	Ga Southern	336 : 33
4.03	Policy Owner	revise	documents	documents upon feedback from advisory committees within 24-48 hours of feedback.	Choice	R	Ga Southern	474 : 7
4.01	Officer(s) of Primary Responsibility (OPR) / Officer(s) of Coordinating Responsibility (OCR)	present	draft policy	typically 30 days for consideration by President's Cabinet and relevant audiences	Information	R	Ga Southern	336 : 31
4.01	Officer(s) of Primary Responsibility (OPR) / Officer(s) of Coordinating Responsibility (OCR)	present	draft policy	typically 30 days for consideration by President's Cabinet and relevant audiences	Information	R	Ga Southern	336 : 31
4.03	Policy Owners	accept	stakeholder input	anytime in the cycle	Information	R	Ga Southern	473 : 2
4.03	Officer(s) of Primary Responsibility (OPR) /	address	requests	for additional information, clarifications, objections, recommendations, etc.	Information	R	Ga Southern	336 : 32

Appendix U Get Approval Rules - Filtered

ACUPA	A	I	B	C	RULE TYPE	DEONTIC	ORG	REF
	Officer(s) of Coordinating Responsibility (OCR)							
4.03	Team	deliver	viable policy drafts	frequently during the development process.	Information	R	Ga Southern	473 : 3
4.04	OPR (CIO)	seek	policy approval	from President's Cabinet by submitting amended draft with date and version accordingly	Information	R	Ga Southern	336 : 35
4.03	Policy Owners	satisfy	the stakeholders	through timely and continuous policy actions	Scope	R	Ga Southern	473 : 1
4.04	President of the Georgia Institute of Technology	[provide]	final approval of this policy	based on a review by the Information Security Policy Committee	Aggregation	R	GT	348 : 8
4.02	PRC	review	new policies, which will be written by OIT-IS	prior to CIO approval and policy publication	Choice	R	GT	360 : 15
4.02	PRC Members	compile	final draft	At the end of 1 month, taking into account the various inputs and recommendations.	Choice	R	GT	360 : 34
4.01	PCM	keep apprised (or apprise)	PRC	of the discussions with the CIO and any changes that are proposed	Information	R	GT	360 : 37
4.03	Information Security Office	present	final draft	to Faculty Executive Board prior to seeking approval.	Information	R	GT	476 : 8
4.03	Information Security Office	meet	faculty senate committee	to review draft	Information	R	GT	476 : 7
4.03	PCM	pass	approved PRC draft	to the CIO for approval.	Information	R	GT	360 : 35
4.03	PCM	brief	CIO	on the proposed changes or new policy	Information	R	GT	360 : 36
4.03	PCM	take	recommendations the CIO has	into account	Information	R	GT	360 : 36.1
4.02	PRC	review	changes	Grammatical, format, or minor (e.g. contact information)	Scope	F	GT	360 : 16

Appendix V Information Rules

ACUPA	A	I	B	C	Organization	ref	Deontic
3.03	the CISO	socialize	the policy/issue and plan	with most of the affected parties during the drafting to help gain support for the policy change	UGA	472 : 21	R
2.10	IT Directors	deliver	Memoranda	regarding Statement of Policy Need	Ga Southern	336 : 10	R
3.03	Team	exchange	information	in face-to-face meetings as much as possible	Ga Southern	473 : 6	R
3.03	Officer(s) of Primary Responsibility (OPR) / Officer(s) of Coordinating Responsibility (OCR)	distribute	policy concept document	to all stakeholders	Ga Southern	336 : 19	R
3.03	Officer(s) of Primary Responsibility (OPR) / Officer(s) of Coordinating Responsibility (OCR)	solicit	input	from all stakeholders [regarding draft policy concept document]	Ga Southern	336 : 20	R
3.03	Officer(s) of Primary Responsibility (OPR) / Officer(s) of Coordinating Responsibility (OCR)	inform	stakeholders	[when distributing policy concept document] of possible changes to policies	Ga Southern	336 : 21	R
3.03	Officer(s) of Primary Responsibility (OPR) / Officer(s) of Coordinating Responsibility (OCR)	inform	stakeholders	[when distributing policy concept document] how it affects them	Ga Southern	336 : 22	R
4.01	Officer(s) of Primary	present	draft policy	typically 30 days for consideration by President's Cabinet and relevant audiences	Ga Southern	336 : 31	R

Appendix V Information Rules

ACUPA	A	I	B	C	Organization	ref	Deontic
4.01	Officer(s) of Primary Responsibility (OPR) / Officer(s) of Coordinating Responsibility (OCR)	present	draft policy	typically 30 days for consideration by President's Cabinet and relevant audiences	Ga Southern	336 : 31	R
4.03	Policy Owners	accept	stakeholder input	anytime in the cycle	Ga Southern	473 : 2	R
4.03	Team	deliver	viable policy drafts	frequently during the development process.	Ga Southern	473 : 3	R
4.03	Officer(s) of Primary Responsibility (OPR) / Officer(s) of Coordinating Responsibility (OCR)	address	requests	for additional information, clarifications, objections, recommendations, etc.	Ga Southern	336 : 32	R
4.04	OPR (CIO)	seek	policy approval	from President's Cabinet by submitting amended draft with date and version accordingly	Ga Southern	336 : 35	R
5.02	Officer(s) of Coordinating Responsibility (OCR)	post	the policy and procedures	to VPIT policy website Once approved,	Ga Southern	336 : 37	R
5.03	Officer(s) of Coordinating Responsibility (OCR)	post	approved policy	in master repository ensuring proper classification for easy reference	Ga Southern	336 : 40	R
5.04	Officer(s) of Coordinating Responsibility (OCR)	distribute	the policy and procedures	Once approved, according to the established communication plan	Ga Southern	336 : 39	R

Appendix V Information Rules

ACUPA	A	I	B	C	Organization	ref	Deontic
5.04	Officer(s) of Coordinating Responsibility (OCR)	distribute	the policy and procedures	Once approved, according to the established communication plan	Ga Southern	336 : 39	R
5.04	Officer(s) of Coordinating Responsibility (OCR)	distribute	policy document	as per communication plan	Ga Southern	336 : 41	R
6.02	Officer(s) of Coordinating Responsibility (OCR)	Communicate	policy retirement	as per Communication Plan	Ga Southern	336 : 54	R
3.03	CISO	present	draft	to Internal Audits for comments	GSU	470 : 9	R
3.03	CISO	present	draft policy	to CIO	GSU	470 : 10	R
4.01	[Team]	submit	policy drafts	to the Office of Institutional Effectiveness	GSU	475 : 6	R
4.01	CIO	present	draft policy	to Admin Council	GSU	470 : 12	R
4.03	The Policy Advisory Group	return	draft policy document	to the Responsible Office/Senate Committee for scheduling the discussion of the policy on the University Senate Agenda.	GSU	475 : 17	R
5.02	[University]	make available	applicable documents	at points of use relevant versions	GSU	367 : 9	R
5.02	The Associate Provost	post	the approved policy.	on the University Website	GSU	475 : 33	R
5.04	The Responsible Office or Senate Committee	notify	relevant individuals and departments	of the policy change.	GSU	475 : 24	R
5.04	[Information Security Department]	make aware	All relevant personnel	of the relevance and importance of their information security activities and how they contribute to the achievement of the ISMS objectives	GSU	367 : 27	R
5.04	The Responsible Ofice	notify	relevant individuals and departments	of the policy change	GSU	475 : 34	R
6.01	[Information Security Department]	include	A revision level showing the new document(s)/version(s)	When a new procedure, or version of a procedure, is issued for inclusion in the University's Information Security Management System	GSU	367 : 10	R

Appendix V Information Rules

ACUPA	A	I	B	C	Organization	ref	Deontic
6.01	[Information Security Department]	include	Point(s) of contact for questions or comments	When a new procedure, or version of a procedure, is issued for inclusion in the University's Information Security Management System	GSU	367 : 11	R
6.01	[Information Security Department]	include	Date of last update or issuance	When a new procedure, or version of a procedure, is issued for inclusion in the University's Information Security Management System	GSU	367 : 12	R
6.01	[Information Security Department]	include	Data classification (if sensitive or confidential)	When a new procedure, or version of a procedure, is issued for inclusion in the University's Information Security Management System	GSU	367 : 13	R
6.03	[Information Security Department]	hold	meetings	for management reviews semiannually	GSU	367 : 18	R
6.04	[Information Security Department]	include	Results of ISMS audits and reviews	in the management reviews	GSU	367 : 19	R
6.04	[Information Security Department]	include	Feedback from interested parties	in the management reviews	GSU	367 : 20	R
6.04	[Information Security Department]	include	Techniques, products or procedures, which could be used at the University to improve the ISMS's performance and effectiveness	in the management reviews	GSU	367 : 21	R
6.04	[Information Security Department]	include	Status of preventive and corrective actions	in the management reviews	GSU	367 : 22	R
6.04	[Information Security Department]	include	Vulnerabilities or threats not adequately	in the management reviews	GSU	367 : 23	R

Appendix V Information Rules

ACUPA	A	I	B	C	Organization	ref	Deontic
6.04	[Information Security Department]	include	addressed in the previous risk assessments Results from effectiveness measurements	in the management reviews	GSU	367 : 24	R
6.04	[Information Security Department]	include	Follow-up actions from previous management reviews	in the management reviews	GSU	367 : 25	R
1.01	Information Security Office	meet	data stewards and/or policy owners	to scan for issues that need to be addressed by policy change	GT	476 : 3	R
2.00	PRC	provide	feedback and constructive criticism	for proposed OIT and GT Security Policies based on their respective functional areas.	GT	360 : 13	R
2.01	IS Policy and Compliance Manager (PCM)	kick off	policy process	when the IS Policy and Compliance Manager (PCM) receives the request to review a policy or write a new policy.	GT	360 : 21	S
2.07	PCM	seek	input	from the various technical communities on campus (GTITC, CSS, CSR's, while writing the new policy or updating existing policies	GT	360 : 27	R
2.09	PCM	forward	information	to the OIT IS Director for preliminary approval to proceed.	GT	360 : 25	R
3.02	PCM	include	summary of proposed changes or new policy highlights	with the draft.	GT	360 : 29	R
3.03	PCM	send	initial draft	to the PRC for review.	GT	360 : 28	R
3.03	PCM	socialize	draft	with various groups (e.g. SGA, Faculty and Technical Leads) for feedback where appropriate	GT	360 : 30	R
3.04	CIO	vet	proposal	with executive leadership team	GT	476 : 1	P
3.04	Information Security Office	vet	proposal	with faculty excutive board, faculty senate, and all units of the campus	GT	476 : 2	R
3.04	Information Security Office	solicit	information	from campus units after proposal/need vetted with executive leadership	GT	476 : 4	R

Appendix V Information Rules

ACUPA	A	I	B	C	Organization	ref	Deontic
3.04	Information Security Office	meet	associate dean and IT director for a campus unit	to discuss changes	GT	476 : 6	R
3.04	Information Security Office	vet	policy proposal	with HR, Legal Affairs prior to vetting with campus units	GT	476 : 11	R
3.05	PRC	handle	initial discussion	During this time, over email with weekly face-face meetings as needed.	GT	360 : 32	R
3.05	PRC Members	are	input	expected to provide input based on their functional areas.	GT	360 : 33	S
4.01	PCM	keep apprised (or apprise)	PRC	of the discussions with the CIO and any changes that are proposed	GT	360 : 37	R
4.03	Information Security Office	meet	faculty senate committee	to review draft	GT	476 : 7	R
4.03	Information Security Office	present	final draft	to Faculty Executive Board prior to seeking approval.	GT	476 : 8	R
4.03	PCM	pass	approved PRC draft	to the CIO for approval.	GT	360 : 35	R
4.03	PCM	brief	CIO	on the proposed changes or new policy	GT	360 : 36	R
4.03	PCM	take	recommendations the CIO has	into account	GT	360 : 36.1	R
5.01	The responsible university officer	notify via email and/or in writing	associate vice provosts; deans, associate vice presidents, unit heads, internal auditing, office of legal affairs, OIT information security, technical leads	upon approval of the policy and upon any subsequent revisions or amendments made to the original document	GT	343 : 187	R
5.02	[Institute]	publish	this policy	upon approval on the Georgia Tech website	GT	344 : 71	O
5.02	PCM	communicate	final document	via email to the campus, once the draft or changes have been approved	GT	360 : 38	R
5.02	PCM	update and post	final draft	to the OIT Policy Website, once the CIO has approved the final draft	GT	360 : 39	R

Appendix V Information Rules

ACUPA	A	I	B	C	Organization	ref	Deontic
5.02	The responsible university officer	publish on the Georgia Tech website	this policy	upon approval	GT	343 : 186	R
5.04	OIT-IS	notify	CIO	of the changes [grammatical, format, or minor] and publish them as necessary.	GT	360 : 17	R
5.04	Georgia Tech Academic and Administrative units, including OIT,	commun icate	this policy	to their users	GT	353 : 26	R
5.04	OIT-IS	publish	this policy	upon approval	GT	353 : 29	R
6.04	Georgia Tech Academic and Administrative units, including OIT,	submit	risk exception requests	via the approved process	GT	353 : 27	R
6.05	OIT-IS	notify	the following groups: OIT, Campus Deans and Chairs, Unit Business/Adminis trative Leads, Georgia Tech IT directors, ITAC, Campus CSR's, Internal Audit	via email and/or in writing upon approval of the standard and upon subsequent reviewsion or amendmnets made to the original document	GT	353 : 30	R
6.05	The responsible university officer	commun icate	Any changes to the policy or procedures	promptly to the individuals and offices noted in section 8	GT	343 : 185	R

Appendix W Scope Rules

ACUPA	A	I	B	C	Organization	ref	Deontic
2.02	Departments, units, or service providers	develop	stricter standards	for themselves with or without the advice or assistance of the CIO and CISO.	UGA	381 : 11	P
2.10	each University System of Georgia institution	develop	policy	authorized by BOR Appropriate Use Policy (2009-14) that, at minimum, includes the Board policy guidelines.	Ga Southern	332 : 3	R
4.03	Policy Owners	satisfy	the stakeholders	through timely and continuous policy actions	Ga Southern	473 : 1	R
2.10	[GT organizations]	reduce	minimum requirements established in this policy	[in] Other policies, standards, procedures, and safeguards documents	GT	344 : 14	F
2.10	[GT organizations]	augment	restrictions	for the sake of security [in] Other policies, standards, procedures, and safeguards documents	GT	343 : 13	P
2.10	[GT]	submit	policy	to applicable federal and State statutes and regulations that guarantee either protection or accessibility of Institute records [will take precedence over this policy]	GT	344 : 5	R
2.10	[GT]	submit	policy	to applicable federal and State statutes and regulations that guarantee either protection or accessibility of Institute records [will take precedence over this policy]	GT	344 : 5	R
4.02	PRC	review	changes	Grammatical, format, or minor (e.g. contact information)	GT	360 : 16	F
7.00	Campus Units	supersede	institutional policy	with their policy.	GT	476 : 5	F

References

Agrawal, Arun. 2014. “Studying the Commons, Governing Common-Pool Resource Outcomes: Some Concluding Thoughts.” *Environmental Science & Policy*, Interrogating The Commons, 36 (February): 86–91. doi:10.1016/j.envsci.2013.08.012.

Albrechtsen, Eirik. 2007. “A Qualitative Study of Users’ View on Information Security.” *Computers & Security* 26 (4): 276–89. doi:doi: DOI: 10.1016/j.cose.2006.11.004.

Aligica, Paul Dragos. 2006. “Institutional and Stakeholder Mapping: Frameworks for Policy Analysis and Institutional Change.” *Public Organization Review* 6 (1): 79–90. doi:10.1007/s11115-006-6833-0.

Aligica, Paul Dragos, and Peter J. Boettke. 2009. *Challenging Institutional Analysis and Development: The Bloomington School*. Routledge.

Ali, Syed Mubashir, Tariq Rahim Soomro, and Muhammad Nawaz Brohi. 2013. “Mapping Information Technology Infrastructure Library with Other Information Technology Standards and Best Practices.” *Journal of Computer Science* 9 (9): 1190–96.

Anderies, J.M, M.A. Janssen, and Elinor Ostrom. 2004. “A Framework to Analyze the Robustness of Social-Ecological Systems from an Institutional Perspective.” *Ecology and Society* 9 (1): 18.

Anderson, Evan E., and Joobin Choobineh. 2008. “Enterprise Information Security Strategies.” *Computers & Security* 27 (1-2): 22–29. doi:doi: DOI: 10.1016/j.cose.2008.03.002.

Anderson, Ross, and Tyler Moore. 2009. “Information Security: Where Computer Science, Economics and Psychology Meet.” *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* 367 (1898): 2717–27. doi:10.1098/rsta.2009.0027.

Andersson, Krister, and Elinor Ostrom. 2008. “Analyzing Decentralized Resource Regimes from a Polycentric Perspective.” *Policy Sciences* 41 (1): 71–93. doi:10.1007/s11077-007-9055-6.

Ansell, Chris, and Alison Gash. 2008. “Collaborative Governance in Theory and Practice.” *Journal of Public Administration Research and Theory* 18 (4): 543–71. doi:10.1093/jopart/mum032.

Appari, Ajit, M. Eric Johnson, and Denise L. Anthony. 2009. “HIPAA Compliance: An Institutional Theory Perspective.” In *AMCIS 2009 Proceedings*. Association for Information Systems. http://www.ists.dartmouth.edu/library/489.pdf.

Arnold, Gwen, and Forrest D. Fleischman. 2013. “The Influence of Organizations and Institutions on Wetland Policy Stability: The Rapanos Case.” *Policy Studies Journal* 41 (2): 343–64. doi:10.1111/psj.12020.

Asosheh, A., P. Hajinazari, and H. Khodkari. 2013. “A Practical Implementation of ISMS.” In *2013 7th Intenational Conference on E-Commerce in Developing Countries: With Focus on E-Security (ECDC)*, 1–17. doi:10.1109/ECDC.2013.6556730.

Backhouse, J, and G Dhillon. 1996. “Structures of Responsibility and Security of Information Systems.” *European Journal of Information Systems* 5 (1): 2–9. doi:10.1057/ejis.1996.7.

Bakari, Jabiri Kuwe, Charles N. Tarimo, Louise Yngstrm, Christer Magnusson, and Stewart Kowalski. 2007. “Bridging the Gap between General Management and Technicians - A Case Study on ICT Security in a Developing Country.” *Computers & Security* 26 (1): 44–55. doi:doi: DOI: 10.1016/j.cose.2006.10.007.

Bardach, Eugene. 1998. *Getting Agencies to Work Together: The Practice and Theory of Managerial Craftsmanship*. Washington, D.C: Brookings Institution Press.

Bartell, Marvin. 2003. “Internationalization of Universities: A University Culture-Based Framework.” *Higher Education* 45 (1): 43–70. doi:10.1023/A:1021225514599.

Baskerville, Richard. 2006. “The Information Security Standards Marketplace.” In *ACIS 2006 Proceedings*, Year 2006:10. Adelaide: Association for Information Systems. http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1085&context=acis2006.

Baskerville, Richard, and Gurpreet Dhillon. 2008. “Information Systems Security Strategy: A Process View.” In *Information Security: Policy, Processes, and Practices*, edited by Detmar W Straub, Seymour E Goodman, and Richard Baskerville. Advances in Management Information Systems. Armonk, N.Y: M.E. Sharpe.

Baskerville, Richard, and Mikko Siponen. 2002. “An Information Security Meta-Policy for Emergent Organizations.” *Logistics Information Management* 15 (5/6): 337–46.

Basurto, Xavier, Gordon Kingsley, Kelly McQueen, Mshadoni Smith, and Christopher M. Weible. 2009. “A Systematic Approach to Institutional Analysis: Applying Crawford and Ostrom’s Grammar.” *Political Research Quarterly*, April, 1065912909334430. doi:10.1177/1065912909334430.

———. 2010a. “A Systematic Approach to Institutional Analysis: Applying Crawford and Ostrom’s Grammar.” *Political Research Quarterly* 63 (3): 523–37. doi:10.2307/25747956.

———. 2010b. “A Systematic Approach to Institutional Analysis: Applying Crawford and Ostrom’s Grammar.” *Political Research Quarterly* 63 (3): 523–37.

Berardo, Ramiro. 2009. “Processing Complexity in Networks: A Study of Informal Collaboration and Its Effect on Organizational Success.” *Policy Studies Journal* 37 (3): 521–39. doi:10.1111/j.1541-0072.2009.00326.x.

Beznosov, Konstantin, and Olga Beznosova. 2007. “On the Imbalance of the Security Problem Space and Its Expected Consequences.” *Information Management & Computer Security* 15 (5): 420–31. doi:10.1108/09685220710831152.

Bjorck, F. 2004. “Institutional Theory: A New Perspective for Research into IS/IT Security in Organisations.” In *Proceedings of the 37th Annual Hawaii International Conference on System Sciences, 2004*. IEEE. doi:10.1109/HICSS.2004.1265444.

Blau, Peter Michael. 1974. *On the Nature of Organizations*. Wiley.

———. 1994. *The Organization of Academic Work*. Transaction Publishers.

Blomquist, William, and Peter deLeon. 2011. “The Design and Promise of the Institutional Analysis and Development Framework.” *Policy Studies Journal* 39 (1): 1–6. doi:10.1111/j.1541-0072.2011.00402.x.

Blomquist, William, and Elinor Ostrom. 2008. “Deliberation, Learning, and Institutional Change: The Evolution of Institutions in Judicial Settings.” *Consitutional Political Economy* 19 (3): 180–202. doi:10.1007/s10602-008-9045-5.

Bohme, Rainer, and Gaurav Kataria. 2006. “Models and Measures for Correlation in Cyber-Insurance.” In . Cambridge [England]. http://weis2006.econinfosec.org/docs/16.pdf.

Bradburn, Norman M. 2004. *Asking Questions: The Definitive Guide to Questionnaire Design: For Market Research, Political Polls, and Social and Health Questionnaires*. Rev. ed. San Francisco: Jossey-Bass.

Bryson, John M., Barbara C. Crosby, and Melissa Middleton Stone. 2015. “Designing and Implementing Cross-Sector Collaborations: Needed and Challenging.” *Public Administration Review* 75 (5): 647–63. doi:10.1111/puar.12432.

Buchan, Nancy R., Gianluca Grimalda, Rick Wilson, Marilynn Brewer, Enrique Fatas, and Margaret Foddy. 2009. “Globalization and Human Cooperation.” *Proceedings of*

the National Academy of Sciences 106 (11): 4138–42. doi:10.1073/pnas.0809522106.

Bulgurcu, Burcu, Hasan Cavusoglu, and Izak Benbasat. 2010. "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness." *MIS Quarterly* 34 (3): 523–A7.

Calanni, John C., Saba N. Siddiki, Christopher M. Weible, and William D. Leach. 2014. "Explaining Coordination in Collaborative Partnerships and Clarifying the Scope of the Belief Homophily Hypothesis." *Journal of Public Administration Research and Theory*, May, mut080. doi:10.1093/jopart/mut080.

Carlsson, L. 2000. "Policy Networks as Collective Action." *POLICY STUDIES JOURNAL* 28 (3): 502–20.

Carter, David P., Christopher M. Weible, Saba N. Siddiki, Xavier Basurto, and Sara Miller Chonaiew. 2013. "Introducing Formal Institutional Analysis of Policy Designs: The Case of the U.S. National Organic Program." In *Sharpening Our Tools in Analyzing Program Designs*. Baltimore. MD.

Carter, David P., Christopher M. Weible, Saba N. Siddiki, John Brett, and Sara Miller Chonaiew. 2015. "Assessing Policy Divergence: How to Investigate the Differences Between a Law and a Corresponding Regulation." *Public Administration* 93 (1): 159–76. doi:10.1111/padm.12120.

Chang, Kuo-chung, and Chih-ping Wang. 2011. "Information Systems Resources and Information Security." *Information Systems Frontiers* 13 (4): 579–93. doi:http://dx.doi.org.prx.library.gatech.edu/10.1007/s10796-010-9232-6.

Chang, Shuchih Ernest, and Chienta Bruce Ho. 2006. "Organizational Factors to the Effectiveness of Implementing Information Security Management." *Industrial Management + Data Systems* 106 (3): 345–61. doi:http://dx.doi.org.prx.library.gatech.edu/10.1108/02635570610653498.

Chang, Shuchih Ernest, and Chin-Shien Lin. 2007. "Exploring Organizational Culture for Information Security Management." *Industrial Management & Data Systems* 107 (3): 438–58. doi:10.1108/02635570710734316.

Chan, Mark, Irene Woon, and Atreyi Kankanhalli. 2005. "Perceptions of Information Security in the Workplace: Linking Information Security Climate to Compliant Behavior." *Journal of Information Privacy & Security* 1 (3): 18–41.

Christensen, Tom. 2010. "University Governance Reforms: Potential Problems of More Autonomy?" *Higher Education*. http://link.springer.com/article/10.1007/s10734-010-9401-z/fulltext.html.

Clement, F, and JM Amezaga. 2008. “Linking Reforestation Policies with Land Use Change in Northern Vietnam: Why Local Factors Matter.” *GEOFORUM* 39 (1): 265–77. doi:10.1016/j.geoforum.2007.05.008.

Cohen, Michael D., James G. March, and Johan P. Olsen. 1972. “A Garbage Can Model of Organizational Choice.” *Administrative Science Quarterly* 17 (1): 1. doi:10.2307/2392088.

Cole, Daniel H., Graham Epstein, and Michael D. McGinnis. 2014. “Digging Deeper into Hardin’s Pasture: The Complex Institutional Structure of ‘the Tragedy of the Commons.’” *Journal of Institutional Economics* 10 (03): 353–69. doi:10.1017/S1744137414000101.

Coleman, James S. 1986. “Social Theory, Social Research, and a Theory of Action.” *The American Journal of Sociology* 91 (6): 1309–35.

Collier, David, and James Mahoney. 1996. “Research Note: Insights and Pitfalls: Selection Bias in Qualitative Research.” *World Politics* 49 (1): 56–91. doi:10.1353/wp.1996.0023.

Connick, Sarah, and Judith E. Innes. 2003. “Outcomes of Collaborative Water Policy Making: Applying Complexity Thinking to Evaluation.” *Journal of Environmental Planning and Management* 46 (2): 177–97. doi:10.1080/0964056032000070987.

Crawford, Sue E. S., and Elinor Ostrom. 1995. “A Grammar of Institutions.” *The American Political Science Review* 89 (3): 582–600.

D’Arcy, John, and Tejaswini Herath. 2011. “A Review and Analysis of Deterrence Theory in the IS Security Literature: Making Sense of the Disparate Findings.” *European Journal of Information Systems* 20 (6): 643–58. doi:10.1057/ejis.2011.23.

D’Arcy, John, and Anat Hovav. 2008. “An Integrative Framework for the Study of Information Security Management Research.” In *Handbook of Research on Information Security and Assurance*, edited by Jatinder N. D. Gupta and Sushil K. Sharma, 55–67. Idea Group Inc (IGI).

da Veiga, Adéle, and Nico Martins. 2015. “Improving the Information Security Culture through Monitoring and Implementation Actions Illustrated through a Case Study.” *Computers & Security* 49 (March): 162–76. doi:10.1016/j.cose.2014.12.006.

deLeon, Peter, and Danielle M. Varda. 2009. “Toward a Theory of Collaborative Policy Networks: Identifying Structural Tendencies.” *Policy Studies Journal* 37 (1): 59–74. doi:10.1111/j.1541-0072.2008.00295.x.

Deutsch, Karl Wolfgang. 1963. *The Nerves of Government; Models of Political Communication and Control*. London: Free Press of Glencoe.

Dhillon, G., and J. Backhouse. 1996. “Risks in the Use of Information Technology within Organizations.” *International Journal of Information Management* 16 (1): 65–74. doi:16/0268-4012(95)00062-3.

Dhillon, Gurpreet, and James Backhouse. 2001. “Current Directions in IS Security Research: Towards Socio-Organizational Perspectives.” *Information Systems Journal* 11 (2): 127–53.

Dhillon, Gurpreet, and Gholamreza Torkzadeh. 2006. “Value-Focused Assessment of Information System Security in Organizations.” *Information Systems Journal* 16 (3): 293–314. doi:10.1111/j.1365-2575.2006.00219.x.

Doherty, Neil F, and Heather Fulford. 2005. “Do Information Security Policies Reduce the Incidence of Security Breaches" An Exploratory Analysis.” *Information Resources Managment Journal* 18 (4): 21–40.

Doherty, Neil F., and Heather Fulford. 2006. “Aligning the Information Security Policy with the Strategic Information Systems Plan.” *Computers & Security* 25 (1): 55–63. doi:10.1016/j.cose.2005.09.009.

Doherty, Neil Francis, Leonidas Anastasakis, and Heather Fulford. 2009. “The Information Security Policy Unpacked: A Critical Study of the Content of University Policies.” *International Journal of Information Management* 29 (6): 449–57. doi:10.1016/j.ijinfomgt.2009.05.003.

———. 2011. “Reinforcing the Security of Corporate Information Resources: A Critical Review of the Role of the Acceptable Use Policy.” *International Journal of Information Management* 31 (3): 201–9. doi:16/j.ijinfomgt.2010.06.001.

Drevin, L., H.A. Kruger, and T. Steyn. 2007. “Value-Focused Assessment of ICT Security Awareness in an Academic Environment.” *Computers & Security* 26 (1): 36–43. doi:doi: DOI: 10.1016/j.cose.2006.10.006.

Dubé, L., and G. Paré. 2003. “Rigor in Information Systems Positivist Case Research: Current Practices, Trends, and Recommendations.” *Mis Quarterly*, 597–636.

Easterby-Smith, Mark. 1997. “Disciplines of Organizational Learning: Contributions and Critiques.” *Human Relations* 50 (9): 1085–1114.

Eeten, Michel, Johannes M. Bauer, John P. M. Groenewegen, and Wolter Lemstra. 2007. “The Economics of Malware.” In . Arlington, CA. http://web.si.umich.edu/tprc/papers/2007/705/Eeten-Bauer-Groenewegen-Lemstra-TPRC-2007.pdf.

Eeten, Michel van, and Johannes M. Bauer. 2009. “Emerging Threats to Internet Security: Incentives, Externalities and Policy Implications.” *Journal of Contingencies and Crisis Management* 17 (4): 221–32. doi:10.1111/j.1468-5973.2009.00592.x.

Eger, Robert, and Justin Marlowe. 2006. “Hofferbert in Transit L A Dynamic Stages Model of the Urban Policy Process.” *Review of Policy Research* 23 (2).

Eisenhardt, Kathleen, and Melissa Graebner. 2007. “Theory Building From Cases: Opportunities and Challenges.” *Academy of Management Journal* 50 (1): 25–32. doi:Article.

Eisenhardt, Kathleen M. 1989. “Building Theories from Case Study Research.” *The Academy of Management Review* 14 (4): 532–50. doi:10.2307/258557.

———. 1991. “Better Stories and Better Constructs: The Case for Rigor and Comparative Logic.” *The Academy of Management Review* 16 (3): 620–27. doi:10.2307/258921.

Elliot, Raymond, Michael O. Young, David Frawley, and M. Lewis Temares. 1991. “Information Security in Higher Education.” Professional Paper Series #5. Boulder Co: CAUSE, The Association for the Management of Information Technology in Higher Education. http://net.educause.edu/ir/library/pdf/PUB3005.pdf.

Elmore, Richard F. 1979. “Backward Mapping: Implementation Research and Policy Decisions.” *Political Science Quarterly* 94 (4): 601–16. doi:10.2307/2149628.

Feiock, Richard C., Christopher M. Weible, David P. Carter, Cali Curley, Aaron Deslatte, and Tanya Heikkila. 2014. “Capturing Structural and Functional Diversity Through Institutional Analysis The Mayor Position in City Charters.” *Urban Affairs Review*, November, 1078087414555999. doi:10.1177/1078087414555999.

Fendt, J., and W. Sachs. 2008. “Grounded Theory Method in Management Research.” *Organizational Research Methods* 11 (3): 430–55.

Flechais, Ivan, and M. Angela Sasse. 2009. “Stakeholder Involvement, Motivation, Responsibility, Communication: How to Design Usable Security in E-Science.” *International Journal of Human-Computer Studies* 67 (4): 281–96. doi:16/j.ijhcs.2007.10.002.

Fulford, Heather, and Neil F Doherty. 2003. “The Application of Information Security Policies in Large UK-Based Organizations: An Exploratory Investigation.” *Information Management and Computer Security* 11 (3): 106–14.

“Georgia Southern University Policies.” 2013. University. *University Policies E-Library*. November 17. http://www.georgiasouthern.edu/policies/.

Giest, Sarah, and Michael Howlett. 2014. “Understanding the Pre-Conditions of Commons Governance: The Role of Network Management.” *Environmental Science & Policy*, Interrogating The Commons, 36 (February): 37–47. doi:10.1016/j.envsci.2013.07.010.

Goel, Sanjay, and InduShobha N Chengalur-Smith. 2010. “Metrics for Characterizing the Form of Security Policies.” *The Journal of Strategic Information Systems* 19 (December): 281–95. doi:http://dx.doi.org/10.1016/j.jsis.2010.10.002.

Goodman, Seymour, and Herbert Lin. 2007. “Toward a Safer and More Secure Cyberspace.” Washington, DC: Committee on Improving Cybersecurity Research in the United States, Computer Science and Telecommunications Board, Division on Engineering and Physical Sciences, National Research Council of the National Academies.

Goo, Jahyun, Myung-Seong Yim, and Dan J. Kim. 2013. “A Path Way to Successful Management of Individual Intention to Security Compliance: A Role of Organizational Security Climate.” SSRN Scholarly Paper ID 2200590. Rochester, NY: Social Science Research Network. http://papers.ssrn.com/abstract=2200590.

Guzman, Indira R., Jeffrey M. Stanton, Kathryn R. Stam, Vibha Vijayasri, Isabelle Yamodo, Nasriah Zakaria, and Cavinda Caldera. 2004. “A Qualitative Study of the Occupational Subculture of Information Systems Employees in Organizations.” In *Proceedings of the 2004 SIGMIS Conference on Computer Personnel Research: Careers, Culture, and Ethics in a Networked Environment*, 74–80. SIGMIS CPR ’04. New York, NY, USA: ACM. doi:10.1145/982372.982388.

Hardin, Garrett. 1968. “The Tragedy of the Commons.” *Science*, New Series, 162 (3859): 1243–48.

Hardy, Scott D., and Tomas M. Koontz. 2009. “Rules for Collaboration: Institutional Analysis of Group Membership and Levels of Action in Watershed Partnerships.” *Policy Studies Journal* 37 (3): 393–414. doi:10.1111/j.1541-0072.2009.00320.x.

Hassebroek, P. 2007. “Institutionalized Environments and Information Security Management: Learning from Y2K: A Comparative Study in a Critical Sector Organization.” Georgia Institute of Technology.

Hatch, Mary Jo. 2006. *Organization Theory: Modern, Symbolic, and Postmodern Perspectives*. 2nd ed. Oxford ; New York: Oxford University Press.

Hawkey, Kirstie, David Botta, Rodrigo Werlinger, Kasia Muldner, Andre Gagne, and Konstantin Beznosov. 2008. “Human, Organizational, and Technological Factors of IT Security.” *CHI ’08 Extended Abstracts on Human Factors in Computing Systems*, CHI EA ’08, , 3639–44.

doi:http://doi.acm.org.www.library.gatech.edu:2048/10.1145/1358628.1358905
.

Heikkila, Tanya. 2015. “Book Review: ‘The Politics of River Basin Organizations: Coalitions, Institutional Design Choices and Consequences.’” *Water Economics and Policy* 01 (03): 1580002. doi:10.1142/S2382624X15800028.

Heinrich, Carolyn, Carolyn Hill, and Laurence Lynn, Jr. 2004. “Governance as an Organizing Theme for Empirical Research.” In *The Art of Governance: Analyzing Management and Administration*, edited by Laurence E. Lynn and Patricia Ingraham. Georgetown University Press.

Hess, Charlotte, and Elinor Ostrom. 2004. “Studying Scholarly Communication: Can Commons Research and the IAD Framework Help Illuminate Complex Dilemmas?” In . Vol. Paper 28. Indiana University: Library and Librarians’ Publication. http://surface.syr.edu/sul/28/.

———. 2007. “An Overview of the Knowledge Commons.” In *Understanding Knowledge as a Commons: From Theory to Practice*, edited by Charlotte Hess and Elinor Ostrom, 3–26. Cambridge, MA: MIT Press. http://dlc.dlib.indiana.edu/archive/00002109/.

Hicklin, Alisa, and Erik Godwin. 2009. “Agents of Change: The Role of Public Managers in Public Policy.” *Policy Studies Journal* 37 (1): 13–20. doi:10.1111/j.1541-0072.2008.00292.x.

Higgins, Huong Ngo. 1999. “Corporate System Security: Towards an Integrated Management Approach.” *Information Management & Computer Security* 7 (5): 217–22. doi:10.1108/09685229910292817.

Höne, Karin, and J. H. P. Eloff. 2002a. “What Makes an Effective Information Security Policy?” *Network Security* 2002 (6): 14–16. doi:16/S1353-4858(02)06011-7.

———. 2002b. “Information Security Policy -- What Do International Information Security Standards Say?” *Computers & Security* 21 (5): 402–9. doi:16/S0167-4048(02)00504-7.

Hong, Kwo-Shing, Yen-Ping Chi, Louis R. Chao, and Jih-Hsing Tang. 2006. “An Empirical Study of Information Security Policy on Information Security Elevation in Taiwan.” *Information Management & Computer Security* 14 (2): 104–15. doi:10.1108/09685220610655861.

Hoover, Kenneth R., and Todd Donovan. 2007. *The Elements of Social Scientific Thinking*. Cengage Learning.

Hsu, Carol, Jae-Nam Lee, and Detmar W. Straub. 2012. “Institutional Influences on Information Systems Security Innovations.” *Information Systems Research* 23 (3-Part-2): 918–39. doi:10.1287/isre.1110.0393.

Hu, Qing, Tamara Dinev, Paul Hart, and Donna Cooke. 2012. “Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture*.” *Decision Sciences* 43 (4): 615–60. doi:10.1111/j.1540-5915.2012.00361.x.

Hu, Qing, Paul Hart, and Donna Cooke. 2007. “The Role of External and Internal Influences on Information Systems Security - a Neo-Institutional Perspective.” *The Journal of Strategic Information Systems* 16 (2): 153–72. doi:16/j.jsis.2007.05.004.

Iachello, Giovanni, and Gregory Abowd. 2008. “Information Security Policy in the US National Context.” In *Information Security : Policy, Processes, and Practices*, edited by Detmar W Straub, Seymour E Goodman, and Richard Baskerville, 231–62. Advances in Management Information Systems. Armonk, N.Y: M.E. Sharpe.

Imperial, Mark T. 1999a. “Analyzing Institutional Arrangements for Ecosystem-Based Management: Lessons from the Rhode Island Salt Ponds SAM Plan.” *Coastal Management* 27 (1): 31–56. doi:10.1080/089207599263884.

———. 1999b. “Institutional Analysis and Ecosystem-Based Management: The Institutional Analysis and Development Framework.” *Environmental Management* 24 (4): 449–65. doi:10.1007/s002679900246.

———. 2005. “Using Collaboration as a Governance Strategy: Lessons From Six Watershed Management Programs.” *Administration Society* 37 (3): 281–320. doi:10.1177/0095399705276111.

“Information Technology Strategic Plan.” 2010. University System of Georgia. http://www.usg.edu/information_technology_services/documents/USG_ITSP2010_2011_final.pdf.

Jochim, Ashley E., and Peter J. May. 2010. “Beyond Subsystems: Policy Regimes and Governance.” *Policy Studies Journal* 38 (2): 303–27. doi:10.1111/j.1541-0072.2010.00362.x.

Jones, Susan, and Katherine Chudoba. 2012. “Information Security Policy Development Through the Lens of the Institutional Analysis and Development Framework.” *WISP 2012 Proceedings* Paper 7 (December). http://aisel.aisnet.org/wisp2012/7.

Kankanhalli, Atreyi, Hock-Hai Teo, Bernard C. Y. Tan, and Kwok-Kee Wei. 2003a. “An Integrative Study of Information Systems Security Effectiveness.” *International*

Journal of Information Management 23 (2): 139–54. doi:16/S0268-4012(02)00105-6.

———. 2003b. "An Integrative Study of Information Systems Security Effectiveness." *International Journal of Information Management* 23 (2): 139–54. doi:16/S0268-4012(02)00105-6.

Karabacak, Bilge, and Ibrahim Sogukpinar. 2006. "A Quantitative Method for ISO 17799 Gap Analysis." *Computers & Security* 25 (6): 413–19. doi:10.1016/j.cose.2006.05.001.

Karyda, Maria, Evangelos Kiountouzis, and Spyros Kokolakis. 2005. "Information Systems Security Policies: A Contextual Perspective." *Computers & Security* 24 (3): 246–60. doi:16/j.cose.2004.08.011.

Katz, Frank. 2005. "The Effect of a University Information Security Survey on Instruction Methods in Information Security." In *Proceedings of the Second Annual Conference on Information Security Curriculum Development*, 43–48. New York: Association for Computing Machinery. doi:10.1145/1107622.1107633.

Kezar, Adrianna. 2006. "The Impact of Institutional Size on Student Engagement." *Journal of Student Affairs Research and Practice* 43 (1). doi:10.2202/1949-6605.1573.

Kiser, Larry, and Elinor Ostrom. 2000. "The Three Worlds of Action: A Metatheoretical Synthesis of Institutional Approaches." In *Polycentric Games and Institutions: Readings from the Workshop in Political Theory and Policy Analysis*, edited by Michael Dean McGinnis. Ann Arbor: University of Michigan Press.

Knapp, Kenneth J., and Claudia J. Ferrante. 2014. "Information Security Program Effectiveness in Organizations: The Moderating Role of Task Interdependence." *Journal of Organizational and End User Computing* 26 (1). http://search.proquest.com.prx.library.gatech.edu/docview/1544858247/F8B4E02F3443443FPQ/2?accountid=11107.

Knapp, Kenneth J., R. Franklin Morris Jr., Thomas E. Marshall, and Terry Anthony Byrd. 2009. "Information Security Policy: An Organizational-Level Process Model." *Computers & Security* 28 (7): 493–508. doi:16/j.cose.2009.07.001.

Knapp, Kenneth J, Thomas E. Marshall, R. Kelly Rainer, and F. Nelson Ford. 2006. "Information Security: Management's Effect on Culture and Policy." *Informatin Management and Computer Security* 14 (1): 24–36.

Knapp, Kenneth J., Thomas E. Marshall, R. Kelly Rainer, and F. Nelson Ford. 2007. "Information Security Effectiveness: Conceptualization and Validation of a Theory." *International Journal of Information Security and Privacy* 1 (2): 20.

Kolkowska, Ella, and Gurpreet Dhillon. 2013. “Organizational Power and Information Security Rule Compliance.” *Computers & Security* 33 (March): 3–11. doi:10.1016/j.cose.2012.07.001.

Koontz, Tomas M. 2005. “We Finished the Plan, So Now What? Impacts of Collaborative Stakeholder Participation on Land Use Policy.” *Policy Studies Journal* 33 (3): 459–81.

Kotulic, Andrew G., and Jan Guynes Clark. 2004. “Why There Aren’t More Information Security Research Studies.” *Information & Management* 41 (5): 597–607. doi:10.1016/j.im.2003.08.001.

Ku, Cheng-Yuan, Yi-Wen Chang, and David C. Yen. 2009. “National Information Security Policy and Its Implementation: A Case Study in Taiwan.” *Telecommunications Policy* 33 (7): 371–84. doi:10.1016/j.telpol.2009.03.002.

Kwon, Myungjung, Frances S. Berry, and Richard C. Feiock. 2009. “Understanding the Adoption and Timing of Economic Development Strategies in US Cities Using Innovation and Institutional Analysis.” *Journal of Public Administration Research and Theory* 19 (4): 967–88. doi:10.1093/jopart/mun026.

Lowery, David. 2002. “Improving Governance.” *Journal of Public Administration Research and Theory* 12 (2): 293–98.

Lubell, Mark. 2015. “Collaborative Partnerships in Complex Institutional Systems.” *Current Opinion in Environmental Sustainability*, Sustainability governance and transformation, 12 (February): 41–47. doi:10.1016/j.cosust.2014.08.011.

Lynn, Laurence E., Carolyn J. Heinrich, and Carolyn J. Hill. 2000. “Studying Governance and Public Management: Challenges and Prospects.” *Journal of Public Administration Research and Theory* 10 (2): 233–62.

———. 2002. “Response to Professor Lowery.” *Journal of Public Administration Research and Theory* 12 (2): 298–302.

May, Jeffrey, and Gaurpreet Dhillon. 2010. “A Holistic Approach for Enriching Information Security Analysis and Security Policy Formation.” *ECIS 2010 Proceedings*, January. http://aisel.aisnet.org/ecis2010/146.

McGinnis, Michael D. 2011a. “An Introduction to IAD and the Language of the Ostrom Workshop: A Simple Guide to a Complex Framework.” *Policy Studies Journal* 39 (1): 169–83.

———. 2011b. “Networks of Adjacent Action Situations in Polycentric Governance.” *Policy Studies Journal* 39 (1): 51–78. doi:10.1111/j.1541-0072.2010.00396.x.

McGinnis, Michael D., and Elinor Ostrom. 2014. “Social-Ecological System Framework: Initial Changes and Continuing Challenges.” *Ecology and Society* 19 (2). doi:10.5751/ES-06387-190230.

Meier, Kenneth J. 2009a. “Policy Theory, Policy Theory Everywhere: Ravings of a Deranged Policy Scholar.” In *Policy Studies Journal*, 37:5–11. Wiley-Blackwell.

———. 2009b. “Policy Theory, Policy Theory Everywhere: Ravings of a Deranged Policy Scholar.” *Policy Studies Journal* 37 (February): 5–11.

Meier, Kenneth J., and Laurence J. O’toole. 2001. “Managerial Strategies and Behavior in Networks: A Model with Evidence from U.S. Public Education.” *Journal of Public Administration Research and Theory* 11 (3): 271–94.

Miles, Matthew B, and A. M Huberman. 1994. *Qualitative Data Analysis: An Expanded Sourcebook*. 2nd ed. Thousand Oaks: Sage Publications.

Millett, John D. 1912-1993. 1962. *The Academic Community; an Essay on Organization.* McGraw-Hill,.

Moellenkamp, Sabine, Machiel Lamers, and Eva Ebenhoeh. 2008. “Institutional Elements for Adaptive Water Management Regimes. Comparing Two Regional Water Management Regimes in the Rhine Basin.” In *Adaptive and Integrated Water Management: Coping with Complexity and Uncertainty*, edited by Claudia Pahl-Wostl, Pavel Kabat, and Jörn Möltgen, 147–66. Springer.

Möllenkamp, Sabine, Machiel Lamers, and Eva Ebenhöh. 2008. “Institutional Elements for Adaptive Water Management Regimes. Comparing Two Regional Water Management Regimes in the Rhine Basin.” In *Adaptive and Integrated Water Management*, 147–66. Springer Berlin Heidelberg. http://dx.doi.org/10.1007/978-3-540-75941-6_8.

Moule, Barry, and Lina Giavara. 1995. “Policies, Procedures and Standards: An Approach for Implementation.” *Information Management & Computer Security* 3 (3): 7–16. doi:10.1108/09685229510092057.

Nicholson-Crotty, Jill, and Kenneth J. Meier. 2003. “Politics, Structure, and Public Policy: The Case of Higher Education.” *Educational Policy* 17 (1): 80–97. doi:10.1177/0895904802239287.

North, Douglass Cecil. 1990. *Institutions, Institutional Change, and Economic Performance*. Cambridge: Cambridge University Press.

Nowlin, Matthew C. 2011. “Theories of the Policy Process: State of the Research and Emerging Trends.” *Policy Studies Journal* 39 (April): 41–60. doi:10.1111/j.1541-0072.2010.00389_4.x.

Orlikowski, Wanda J., and Stephen R. Barley,. 2001. “Technology and Institutions: What Can Research on Information Technology and Research on Organizations Learn from Each Other?” *MIS Quarterly* 25 (2): 145–65.

Ostrom, Elinor. 1990. *Governing the Commons : The Evolution of Institutions for Collective Action /*. The Political Economy of Institutions and Decisions. Cambridge University Press,.

———. 1991. *Governing the Commons: The Evolution of Institutions for Collective Action*. Cambridge [England]: Cambridge University Press.

———. 2005. *Understanding Institutional Diversity*. Princeton: Princeton University Press.

———. 2008a. “Developing a Method for Analyzing Institutional Change.” In *ASSESSING THE EVOLUTION AND IMPACT OF ALTERNATIVE INSTITUTIONAL STRUCTURES*, edited by Sandra Batie and Nicholas Mercuro. London: Routledge Press. http://ssrn.com/paper=997837.

———. 2008b. “Polycentric Systems as One Approach for Solving Collective-Action Problems.” *SSRN eLibrary*. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1304697.

———. 2010. “Beyond Markets and States: Polycentric Governance of Complex Economic Systems.” *American Economic Review* 100 (3): 641–72. doi:10.1257/aer.100.3.641.

———. 2011. “Background on the Institutional Analysis and Development Framework.” *Policy Studies Journal* 39 (1): 7–27. doi:10.1111/j.1541-0072.2010.00394.x.

Ostrom, Elinor, and Xavier Basurto. 2011. “Crafting Analytical Tools to Study Institutional Change.” *Journal of Institutional Economics* 7 (Special Issue 03): 317–43. doi:10.1017/S1744137410000305.

Ostrom, Elinor, and Sue E. S. Crawford. 2005a. “A Grammar of Institutions.” In *Understanding Institutional Diversity*, edited by Elinor Ostrom, 137–74. Princeton: Princeton University Press.

———. 2005b. “Classifying Rules.” In *Understanding Institutional Diversity*, edited by Elinor Ostrom, 186–215. Princeton: Princeton University Press.

Ostrom, Elinor, Roy Gardner, and James Walker. 1994. *Rules, Games, and Common-Pool Resources*. Ann Arbor: University of Michigan Press.

Ostrom, Elinor, and Charlotte Hess. 2007. “A Framework for Analyzing the Knowledge Commons.” In *Understanding Knowledge as a Commons: From Theory to*

Practice, edited by Charlotte Hess and Elinor Ostrom. Cambridge, MA: MIT Press. http://dlc.dlib.indiana.edu/archive/00002109/.

Ostrom, Vincent, Charles M. Tiebout, and Robert Warren. 1961. "The Organization of Government in Metropolitan Areas: A Theoretical Inquiry." *The American Political Science Review* 55 (4): 831–42. doi:10.2307/1952530.

O'Toole Jr., Laurence J. 1997. "Treating Networks Seriously: Practical and Research-Based Agendas in Public Administration." *Public Administration Review* 57 (1): 45–52.

———. 2000. "Research on Policy Implementation: Assessment and Prospects." *J Public Adm Res Theory* 10 (2): 263–88.

———. 2010. "The Ties That Bind? Networks, Public Administration and Political Science." *Political Science and Politics* 43 (1): 7–14. doi:10.1017/S1049096509990576.

O'Toole, Laurence J., and Kenneth J. Meier. 2004. "Public Management in Intergovernmental Networks: Matching Structural Networks and Managerial Networking." *Journal of Public Administration Research and Theory* 14 (4): 469–94. doi:10.1093/jopart/muh032.

O'Toole, Laurence J., and Kenneth J. Meier. 2015. "Public Management, Context, and Performance: In Quest of a More General Theory." *Journal of Public Administration Research and Theory* 25 (1): 237–56. doi:10.1093/jopart/muu011.

O'Toole, L. J. 2004. "The Theory–Practice Issue in Policy Implementation Research." *Public Administration* 82 (2): 309–29.

Pieters, W., T. Dimkov, and D. Pavlovic. 2013. "Security Policy Alignment: A Formal Approach." *IEEE Systems Journal* 7 (2): 275–87. doi:10.1109/JSYST.2012.2221933.

Portnoy, Michael, and Seymour Goodman, eds. 2009. *Global Initiatives to Secure Cyberspace: An Emerging Landscape*. New York: Springer Science+Business Media.

Posthumus, Shaun, and Rossouw von Solms. 2004. "A Framework for the Governance of Information Security." *Computers & Security* 23 (8): 638–46. doi:16/j.cose.2004.10.006.

Provan, KG, and P Kenis. 2008. "Modes of Network Governance: Structure, Management, and Effectiveness." *JOURNAL OF PUBLIC ADMINISTRATION RESEARCH AND THEORY* 18 (2): 229–52. doi:10.1093/jopart/mum015.

Purvis, Russell L., V. Sambamurthy, and Robert W. Zmud. 2001. “The Assimilation of Knowledge Platforms in Organizations: An Empirical Investigation.” *Organization Science* 12 (2): 117–35. doi:10.1287/orsc.12.2.117.10115.

Raab, Jörg, Remco S. Mannak, and Bart Cambré. 2015. “Combining Structure, Governance, and Context: A Configurational Approach to Network Effectiveness.” *Journal of Public Administration Research and Theory* 25 (2): 479–511. doi:10.1093/jopart/mut039.

Ramachandran, S., S.V. Rao, and T. Goles. 2008. “Information Security Cultures of Four Professions: A Comparative Study.” In *Hawaii International Conference on System Sciences, Proceedings of the 41st Annual*, 454–454. doi:10.1109/HICSS.2008.201.

Ramanauskaite, Simona, Dmitrij Olifer, Nikolaj Goranin, and Antanas Čenys. 2013. “Security Ontology for Adaptive Mapping of Security Standards.” *International Journal of Computers Communications & Control* 8 (6): 878–90. doi:10.15837/ijccc.2013.6.764.

Rees, Jackie, Subhajyoti Bandyopadhyay, and Eugene H. Spafford. 2003. “PFIRES: A Policy Framework for Information Security.” *Commun. ACM* 46 (7): 101–6. doi:10.1145/792704.792706.

Reichman, Henry, Ashley Dawson, Martin Garnar, Chris Hoofnagle, Rana Jaleel, Anne Klinefelter, Robert O’Neil, and Jennifer Nichols. 2014. “Academic Freedom and Electronic Communications.” *Journal of Collective Bargaining in the Academy*, no. 9 (September). http://thekeep.eiu.edu/jcba/vol0/iss9/20.

Rezgui, Yacine, and Adam Marks. 2008. “Information Security Awareness in Higher Education: An Exploratory Study.” *Computers & Security* 27 (7-8): 241–53. doi:doi: DOI: 10.1016/j.cose.2008.07.008.

Robichau, Robbie Waters. 2011. “The Mosaic of Governance: Creating a Picture with Definitions, Theories, and Debates.” *Policy Studies Journal* 39 (April): 113–31. doi:10.1111/j.1541-0072.2010.00389_8.x.

Robichau, Robbie Waters, and Laurence E. Lynn Jr. 2009. “The Implementation of Public Policy: Still the Missing Link.” *Policy Studies Journal* 37 (1): 21–36.

Rowlingson, Robert, and Richard Winsborrow. 2006. “A Comparison of the Payment Card Industry Data Security Standard with ISO17799.” *Computer Fraud & Security* 2006 (3): 16–19. doi:10.1016/S1361-3723(06)70323-2.

Sabatier, Paul A. 2007a. “The Need for Better Theories.” In *Theories of Policy Process*. Boulder, Colo: Westview Press.

———. , ed. 2007b. *Theories of Policy Process*. Boulder, Colo: Westview Press.

Sabherwal, Rajiv, and Yolande E. Chan. 2001. “Alignment Between Business and IS Strategies: A Study of Prospectors, Analyzers, and Defenders.” *Information Systems Research* 12 (1): 11–33. doi:10.1287/isre.12.1.11.9714.

Sandstrom, Annica, and Lars Carlsson. 2008. “The Performance of Policy Networks: The Relation between Network Structure and Network Performance.” *Policy Studies Journal* 36 (4): 497–524.

Sangseo Park, A. Ahmad, and A. B Ruighaver. 2010. “Factors Influencing the Implementation of Information Systems Security Strategies in Organizations.” In *2010 International Conference on Information Science and Applications (ICISA)*, 1–6. IEEE. doi:10.1109/ICISA.2010.5480261.

Seidenfeld, Mark. 2000. “Empowering Stakeholders: Limits on Collaboration as the Basis for Flexible Regulation.” *William & Mary Law Review* 41 (2): 411.

Siddiki, Saba, Xavier Basurto, and Chris Weible. 2010. “Comparing Formal and Informal Institutions with the Institutional Grammar Tool.” In . Capturing the Complexity of the Commons, North American Regional Meeting of the International Association for the Study of the Commons. http://hdl.handle.net/10535/6562.

Siddiki, Saba, Xavier Basurto, and Christopher M. Weible. 2012. “Using the Institutional Grammar Tool to Understand Regulatory Compliance: The Case of Colorado Aquaculture.” *Regulation & Governance* 6 (2): 167–88. doi:10.1111/j.1748-5991.2012.01132.x.

Siddiki, Saba N. 2013. “Assessing Policy Design, Appropriateness, and Coerciveness Using the Institutional Grammar Tool.” In *Sharpening Our Tools in Analyzing Program Designs*. Baltimore. MD.

Siddiki, Saba N., Julia L. Carboni, Chris Koski, and Abdul-Akeem Sadiq. 2015. “How Policy Rules Shape the Structure and Performance of Collaborative Governance Arrangements.” *Public Administration Review*, February, n/a – n/a. doi:10.1111/puar.12352.

Siddiki, Saba, Christopher M. Weible, Xavier Basurto, and John Calanni. 2011. “Dissecting Policy Designs: An Application of the Institutional Grammar Tool.” *Policy Studies Journal* 39 (1): 79–103. doi:10.1111/j.1541-0072.2010.00397.x.

Simon, Herbert A. 1962. “The Architecture of Complexity.” *Proceedings of the American Philosophical Society* 106 (6): 467–82.

Simon, Herbert A. 1964. “On the Concept of Organizational Goal.” *Administrative Science Quarterly* 9 (1): 1. doi:Article.

———. 1973. “The Structure of Ill Structured Problems.” *Artificial Intelligence* 4 (3-4): 181–201. doi:10.1016/0004-3702(73)90011-8.

Singleton, Royce. 1999. *Approaches to Social Research*. 3rd ed. Oxford University Press,.

Siponen, Mikko, and Juhani Iivari. 2006. “Six Design Theories for IS Security Policies and Guidelines.” *Journal of the Association for Information Systems* 7 (7): 445–72.

Siponen, Mikko T., and Harri Oinas-Kukkonen. 2007. “A Review of Information Security Issues and Respective Research Contributions.” *SIGMIS Database* 38 (1): 60–80. doi:10.1145/1216218.1216224.

Siponen, Mikko, and Robert Willison. 2009. “Information Security Management Standards: Problems and Solutions.” *Information & Management* 46 (5): 267–70. doi:10.1016/j.im.2008.12.007.

Siponen, M., S. Pahnila, and M.A. Mahmood. 2010. “Compliance with Information Security Policies: An Empirical Investigation.” *Computer* 43 (2): 64–71.

Smith, Stephen, Donald Winchester, Deborah Bunker, and Rodger Jamieson. 2010. “Circuits of Power: A Study of Mandated Compliance to an Information Systems Security De Jure Standard in a Government Organization.” *MIS Quarterly* 34 (3): 463–86.

Stoker, Gerry. 1998. “Governance as Theory: Five Propositions.” *International Social Science Journal* 50 (155): 17–28.

Stoker, Robert Phillip. 1991. *Reluctant Partners: Implementing Federal Policy*. University of Pittsburgh Pre.

Stone, Clarence N. 1998. “Regime Analysis and the Study of Urban Politics, a Rejoinder.” *Journal of Urban Affairs* 20 (3): 249.

Straub, Detmar W., and Richard J. Welke. 1998. “Coping with Systems Risk: Security Planning Models for Management Decision Making.” *MIS Quarterly* 22 (4): 441–69. doi:10.2307/249551.

“The Analysis Suggests That over 94 Percent of the Public Research in Computer Security Has Been Concentrated on Technolo.” n.d.

Thong, James Y. L., Chee-Sing Yap, and K. S. Raman. 1996. “Top Management Support, External Expertise and Information Systems Implementation in Small Businesses.” *Information Systems Research* 7 (2): 248–67. doi:10.1287/isre.7.2.248.

Truex, Duane P., Richard Baskerville, and Heinz Klein. 1999. “Growing Systems in Emergent Organizations.” *Commun. ACM* 42 (8): 117–23. doi:10.1145/310930.310984.

Tversky, Amos, and Daniel Kahneman. 1986. “Rational Choice and the Framing of Decisions.” *The Journal of Business* 59 (4): S251–78.

van Bueren, Ellen M., Erik-Hans Klijn, and Joop F. M. Koppenjan. 2003. “Dealing with Wicked Problems in Networks: Analyzing an Environmental Debate from a Network Perspective.” *J Public Adm Res Theory* 13 (2): 193–212. doi:10.1093/jopart/mug017.

von Solms, Basie. 2005. “Information Security Governance: COBIT or ISO 17799 or Both?” *Computers & Security* 24 (2): 99–104. doi:16/j.cose.2005.02.002.

Wade H. Baker, and Linda Wallace. 2007. “Is Information Security Under Control?: Investigating Quality in Information Security Management.” *Security & Privacy, IEEE* 5 (1): 36–44.

Warkentin, Merrill, and Johnston. 2008. “IT Governance/Organizational Design for Security Management.” In *Information Security: Policy, Processes, and Practices*, edited by Detmar W Straub, Seymour E Goodman, and Richard Baskerville, 46–68. Advances in Management Information Systems. Armonk, N.Y: M.E. Sharpe.

Watkins, Cristy, and Lynne M. Westphal. 2015. “People Don’t Talk in Institutional Statements: A Methodological Case Study of the Institutional Analysis and Development Framework.” *Policy Studies Journal*, November, n/a – n/a. doi:10.1111/psj.12139.

Weber, Edward P., and Anne M. Khademian. 2008. “Wicked Problems, Knowledge Challenges, and Collaborative Capacity Builders in Network Settings.” *Public Administration Review* 68 (2): 334–49.

Weible, Christopher M., and David P. Carter. 2015. “The Composition of Policy Change: Comparing Colorado’s 1977 and 2006 Smoking Bans.” *Policy Sciences* 48 (2): 207–31. doi:http://dx.doi.org.ezproxy.gsu.edu/10.1007/s11077-015-9217-x.

Weible, Christopher M., Paul A. Sabatier, Hank C. Jenkins-Smith, Daniel Nohrstedt, Adam Douglas Henry, and Peter deLeon. 2011. “A Quarter Century of the Advocacy Coalition Framework: An Introduction to the Special Issue.” *Policy Studies Journal* 39 (3): 349–60. doi:10.1111/j.1541-0072.2011.00412.x.

Weible, Christopher M., Saba N. Siddiki, and Jonathan J. Pierce. 2011. “Foes to Friends: Changing Contexts and Changing Intergroup Perceptions.” *Journal of Comparative Policy Analysis: Research and Practice* 13 (5): 499–525. doi:10.1080/13876988.2011.605941.

Weick, Karl E. 1976. “Educational Organizations as Loosely Coupled Systems.” *Administrative Science Quarterly* 21 (1): 1–19. doi:Article.

Werlinger, Rodrigo, Kirstie Hawkey, and Konstantin Beznosov. 2009. “An Integrated View of Human, Organizational, and Technological Challenges of IT Security Management.” *Information Management & Computer Security* 17 (1): 4–19. doi:10.1108/09685220910944722.

Werlinger, Rodrigo, Kirstie Hawkey, David Botta, and Konstantin Beznosov. 2009. “Security Practitioners in Context: Their Activities and Interactions with Other Stakeholders within Organizations.” *International Journal of Human-Computer Studies* 67 (7): 584–606. doi:10.1016/j.ijhcs.2009.03.002.

Whitman, Michael. 2008. “Security Policy: From Design to Maintenance.” In *Information Security : Policy, Processes, and Practices*, edited by Detmar W Straub, Seymour E Goodman, and Richard Baskerville, 123–51. Advances in Management Information Systems. Armonk, N.Y: M.E. Sharpe.

Wiener, Norbert. 1948. *Cybernetics; Or, Control and Communication in the Animal and the Machine.* New York,: J. Wiley.

Yin, Robert K. 2003. *Applications of Case Study Research*. 2nd ed. Applied Social Research Methods Series, v. 34. Thousand Oaks: Sage Publications.

Yin, Robert K. 2009. *Case Study Research: Design and Methods*. SAGE.

Zuccato, Albin. 2007. “Holistic Security Management Framework Applied in Electronic Commerce.” *Computers & Security* 26 (3): 256–65. doi:doi: DOI: 10.1016/j.cose.2006.11.003.