ABSTRACT

Title of Document: **E – GOVERNMENT TECHNICAL SECURITY CONTROLS TAXONOMY FOR INFORMATION ASSURANCE CONTRACTORS – A RELATIONAL APPROACH**

Momodu I. Fofana, Ph.D. in Civil and Environment 2010

Directed By: A. James Clark Chair, Professor Miroslaw J. Skibniewski, Department of Civil and Environmental Engineering

When project managers consider risks that may affect a project, they rarely consider risks associated with the use of information systems. The Federal Information Security Management Act (FISMA) of 2002 recognizes the importance of information security to the economic and national security of the Unites States. The requirements of FISMA are addressed using the NIST Special Publication 800-53 Rev 3, which has improved the way organizations practice information assurance.

The NIST SP 800-53 Rev 3 takes a hierarchical approach to information assurance, which has resulted in the duplication and subsequent withdrawal and merging of fifteen security controls. In addition, the security controls are not associated with the

appropriate information systems. The current security assessment model often results in a waste of resources, since controls that are not applicable to an information system have to be addressed.

This research developed and tested the value of using an information system breakdown structure (ISBS) model for identification of project information system resources. It also assessed the value of using an e-Government Relational Technical Security Controls Model for mapping the ISBS to the applicable relational technical security controls.

A questionnaire containing ninety-five items was developed and emailed to twenty-four information security contractors of which twenty-two efficiently completed questionnaires were received. The questionnaire assessed the value of using the ISBS, and the relationships of the e-Government Relational Technical Security Controls model. Literature review and industry experts opinion was used to triangulate the research results and establish their validity. Cronbach's Alpha coefficient for the four sections of the questionnaire established its reliability.

The results of the research indicated that the ISBS model is an invaluable, customizable, living tool that should be used for identification of information system resources on projects. It can also be used for assigning responsibility for the different information systems and for security classification. The study also indicated that using the e-Government Relational Technical Security Controls provides a relational

and fully integrated approach to information assurance while reducing the likelihood of duplicating security controls. This study could help project managers identify and mitigate risks associated with the use of information systems on projects.

E – GOVERNMENT TECHNICAL SECURITY CONTROLS TAXONOMY FOR INFORMATION ASSURANCE CONTRACTORS – A RELATIONAL APPROACH.

By

Momodu I. Fofana

Dissertation submitted to the Faculty of the Graduate School of the
University of Maryland, College Park, in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
2010

Advisory Committee:
Professor Miroslaw Skibniewski, Chair
Professor Gregory Baecher
Professor Ali Mosleh
Professor Guangming Zhang
Doctor Raghavan Kunigahalli

Dedication

This dissertation is dedicated to my daughter Mariama, for her love, understanding, encouragements, patience and support.

Acknowledgements

I would like to express my sincere gratitude to my dissertation advisor, Prof. Miroslaw J. Skibniewski, for his direction, encouragements and research guidance that has made me the researcher I have become today. Working under his supervision has been a rewarding and stimulating experience. His guidance help me approach my research topic with an objective and exploratory approach for which I am forever thankful. I have also significantly benefited from his knowledge and expertise in my academic and professional life.

I am grateful to my committee members, Prof. Gregory Baecher, Prof. Ali Mosleh, Prof. Guangming Zhang and Dr. Raghavan Kunigahalli, for their reviews, critiques, feedback, questions and valuable guidance throughout my research. I appreciate their guidance in helping me reduce the scope and refocus of my research so that I can be successful. Their recommendations, advice and feedback helped guide the direction of the research.

My special thanks goes to Dr. Sylvion Mbi, my supervisor at work who helped me identify a research topic that is of direct relevance to the information assurance industry. He also acted as a sounding board for my ideas, participated in the pilot testing of my questionnaire, and helped me establish the face value of my questionnaire. Thank you for allowing me to take time away from work so I can concentrate on my literature review in time for the proposal defense. Those days away from work made all the difference.

I would also like to thank Ms. Marianna Swanson of the National Institute of Standards and Technology who pointed me to areas to identify issues facing the NIST Special Publication 800-53.

I would like to extend my sincere appreciation to my respondents who took time of their busy schedule to address my twenty-two page data collection questionnaire and

for sharing their extensive knowledge and expertise in information assurance, without which this research would have been impossible. Respondents who gave approval to be recognized in random order include; Qawi Robinson, Mark Griffith, Michael Turay, Eric Eskelsen, Charles Adefila, Rod Oldenburg, Greg Dagoumas, Jason Marsico, Mansa Leighton-Armah, Patrice Bourgeois, Damon Vermillion, Lillian Day, Terry Benjamin, Jeffrey Coleman, Curtis Lovett, Gibril Koroma, Nadeem Ahmed, Johnathan Vandergriff, Desiree Payne and Wing Chan. I would also like to recognize two other respondents that choose to remain anonymous.

I would like to recognize feedback I received from the e-Construction group that was the sounding board for my presentations and for all the questions they asked that helped me better prepare for my proposal defense and dissertation defense.

I would like to thank my friends and extended family for their understanding during this research. I would also like to acknowledge my mum for her encouragement, eagerness and forever-available ear to discuss the trials and tribulations of the research.

Mariama and Aaron for their love, patience and understanding I would forever be thankful. I want to recognize the help I received from Aaron with babysitting Mariama while I took classes to complete the coursework, prepared for exams and for technical editing of my first and second drafts. Mariama thank you for her endless cups of tea and hugs. I would never have undertaken this journey if I did not have these two very special people in my life. Thank you for everything. I can never thank you enough for all your help.

Table of Contents

List of Figures

List of Tables

Chapter 1 Introduction

1.0 Background and Problem Statement

The events of September 11th, 2001 established the need for the United States Government to revaluate its approach to all aspects of security. A commonly held belief in the Information Security industry is that the outcome of future wars will be determined by the United States Government's ability to keep hackers and other intruders out and ensure the confidentiality, availability and integrity of data, information, information systems and assets.

The Office of Management and Budget Fiscal Year 2008 Report on the implementation of the Federal Information Security Management Act of 2002 states that "In fiscal year 2008, Federal agencies spent $6.2 billion securing the government's total IT investment of approximately $68 billion for the fiscal year of 2008 enacted level, equating to approximately 9.2 percent of the total IT portfolio." Information Technology funds were spent in the following sectors: certification and accreditation of systems, testing of security controls and user awareness training.

Disrupting information systems that support the United States energy, health care, commercial or other critical infrastructure can cause mayhem to the United State's ability to deliver services and products to its citizens and stakeholders. It can also have drastic effects on the financial markets and the ability of the United States to trade with its international trading partners. This can result in marked fluctuations in the value of the US dollar vis-à-vis other currencies, which can affect the US economy, depending on the debt structure. The threat to maintain the US critical infrastructure and ensure the commercial viability of financial markets underscores the importance of information assurance to the US Government.

The ease and low cost required to initiate attacks on the US critical infrastructure, makes this threat a reality. To abate this threat, the United States Government has established regulations and instituted several programs to ensure that threats to its

critical infrastructure are assessed annually, mitigated, accepted, transferred, managed and reported to the United States Congress. In 2002, the US Congress enacted the E-Government Act, which is a requirement for all US Federal Agencies and Federal Government Contractors.

Whitman (2008) summarizes the problem facing the US Government as "The race to keep up with new, more complex and aggressive ways for compromising systems is identified daily." Whitman (2008) maintains that, "The importance of information security is such that it cannot be left exclusively to the hands of the information technology department." I suggest that project managers take an active role in identifying project management best practices for identifying, mitigating and managing the risks posed to the systems that make up the US critical infrastructure.

Operations research teaches us that to minimize the threats posed to the critical infrastructure due to the use of information systems; we must first observe the systems. Determine the risk factors, cost, resources, etc and then develop a verifiable model that can be used to predict the risk behavior and use analytical methods to identify an optimal solution to mitigate the problem.

Project management ensures a project's schedule variances, cost variances and risks are calculated and tracked using Gantt charts, network diagrams, critical path analysis, earned value management and other risk management methodologies. Current project management methodologies identify, assess and mitigating risks to time, quality, cost and customer satisfaction but they do not assess the risk posed by the use of information systems in achieving the goals and objectives of the project.

The National Institute of Science and Technology has developed a three-tiered (High, Moderate and Low) hierarchical security assessment framework for assessing the risk posed by the use of information systems. The problems with this system include the following:

- The security control families are not fully integrated and this result in duplication of control families as is evident from the fifteen security controls that were withdrawn and merged into existing controls for NIST SP 800-53 Rev 3 released on August 2009. To have a robust information system, all the security controls for applications, infrastructure, data, information, information systems and assets should be fully integrated and functioning harmoniously to protect the organization, as an information system is only as robust as its weakest link.
- The NIST security controls assume a one-size-fits-all approach to security assessment, which is not representative of organizational and project security assessment practices. When performing a security assessment of network devices like routers and switches, controls that may not be applicable on to Email Servers still have to be addressed. This often results in extended security assessment and the unnecessary waste of resources by the Federal Government and Contractors.
- Organizations need to wrap project management methodologies around security assessment processes and ensure they are fully integrated with organizational processes, customizable and repeatable.

Information systems are used in the five project management processes yet very little or no attempt has been made to develop a project management methodology that can help with identifying, assessing, mitigating, transferring and managing the risks associated with using information systems on a project.

Keyes (2009) recognizes that "The earlier a risk is identified and dealt with, the less likely it is to negatively affect project outcomes." Keyes also states that risks are probably more easily addressed early on in a project lifecycle. It is much cheaper to make changes to the project in the earlier stages than much later on after most of the funds have been committed. All these conditions indicate that there is a need for early identification and mitigation of project based risks that are associated with the use information systems.

1.1 Research Objective

The objectives for this research include the following:

1. To identify the different information systems that makes up a project environment.
2. To develop an e-Government Technical Controls taxonomy for Federal Government information assurance contractors.
3. To identify effective risk mitigation and management strategies for the identification and authentication controls.
4. To develop a cost model for security assessment of identification and authentication controls.

1.2 Research Questions

The questions that this research shall address include the following:

1. Can we develop an e-Government Technical Controls Relational taxonomy for Federal Government Information Assurance Contractors?
2. What are the effective risk mitigation and management strategies for the Identification and Authentication Security Control Family?
3. What are the associated cost calculations for performing security assessment of the Identification and Authentication Security Control Family?

1.3 The Research Scope

Project management tends to concentrate on the risks associated with cost, quality, timely delivery of the project and customer satisfaction. Yet on most projects, we find that information systems are used to facilitate the initiating, planning, executing, tracking, management and control of project. Very little or no research has been conducted on the risks posed by the use of information systems in project. The risks associated with the use of information systems on a project can cause a project to fail or it may lead to the loss of confidentiality, availability or the integrity of data or information.

A common belief in the field of project management is that 'risks that are identified much later in the project timeline are more difficult to address and likelier to have significant undesirable impact to a project'. A trend is developing wherein the ease of managing risks on projects appears to have some relationship to the time of identification, where the time of identification is measured from the start time of the project. Thus the sooner we start looking at the threats posed by the use of information systems in projects, the sooner we can identify and implement risk mitigation and management strategies that ensure the risk posed by the use of information systems on projects is sufficiently mitigated and managed.

The goal of this research is to develop a relational e-Government Technical Controls taxonomy that can be used to systematically identify, classify, mitigate and manage information systems risks. Early identification and management of information system project threats reduces the likelihood of these risks negatively affecting the project much later in the project life cycle when the costs of the impact can be higher.

Project management research for information systems shows the typical cost model to be a J-shaped chart, which indicates that earlier in the project, there is more flexibility in planning and adjusting project metrics than it is much later in the project cycle. In addition, in the later stages of the project, most of the funds would have been committed and expectations are set.

Project management e-Government Technical Controls taxonomy is a major first step towards developing an invaluable tool for identifying, classifying, mitigating, transferring, accepting and managing information systems risks. This research shall develop an e-Government Technical Controls taxonomy for Federal Government Information Assurance Contractors. This taxonomy will assist information security contractors, project managers, network engineers/administrators and pertinent stakeholders to discuss information systems risk as further emphasized in PMBOK Fourth Edition: "The format of the risk statement should be consistent to ensure the ability to compare the relative effect of one risk against others on the project."

This research will develop, validate and document a fundamental information systems breakdown structure for information systems projects. It will also develop and validate the relationships between the entities of the e-Government Relational Technical Controls and identify effective risks mitigation and management strategies for the identification and authentication control family. It will develop a cost model for performing security assessment for the identification and authentication control family. This taxonomy will facilitate the effective identification and categorization of information system risks so that information security contractors, project managers, network engineers/administrators and pertinent stakeholders can easily reuse them to identifying risks that may affect a project based on its information system components.

This research shall be limited to developing an e-Government Relational Technical Controls taxonomy for project information systems as they relate to the e-Government Technical Controls of the NIST SP 800-53 Rev 3 released in August 2009. It will not develop an e-Government Relational Management taxonomy or an e-Government Relational Operational Controls taxonomy. It will not address the risks posed to virtual machines or associated with ransom-ware, sub-standard organizational processes, information warfare and policy-based security management. The assessment of the current risk mitigation and management strategies is limited to the Identification and Authentication Control Family.

1.4 The Research Methodology

The research effort was partitioned into three phases and executed according to the research methodology depicted in Figure 1.1. Detailed descriptions of the processes involved in each phase of the research methodology are presented in sections 1.5, 1.6 and 1.7.

1.5 PHASE 1: Research Model Development

The researcher conducted an exhaustive literature review in the area of project management for Federal Information Systems Management Act 2002, E-Government Act, information security, information technology, information systems, information assurance, risk management, organizational theory, operations research, statistical tools and prior academic research related to project management of information assurance contracts.

Searches were done on the following online library catalogs; UMCP Library, Montgomery County Library, Project Management Institute (PMI), American Society of Civil Engineers (ASCE), CIO Magazine and Institute of Electrical and Electronics Engineers. The searches included the following words: Taxonomy, vulnerability, risk assessment, security assessment, risk management, risk mitigation, FISMA 2002, e-Government, information assurance, breakdown structure NIST SP, operations management and project risk management. The researcher reviewed publication abstracts and table of contents of textbooks to ensure they are applicable to the research and appropriate for inclusion in the literature review.

Due to the dynamic nature of Information Security, the majority of the books and publications included in this research are those published or written on or after 2006. Materials published prior to 2006 that may have been included in this research were screened for their currency prior to inclusion in this literature review. The researcher continued to review publications in information security and project management magazines to ensure the currency of the research.

The literature was categorized based on the year of publication and its relevance to the research topic. The researcher rejected, or sparingly included material that addressed information security theory but had no relevant associations to project management. These papers also proved to be of very little interest to the researcher and presented very little or no areas for future project management science research.

Information security contractors, network engineers/administrators and project managers with over four years of expertise performing security assessments were interviewed to identify the current challenges when managing information assurance projects. The researcher also utilized his extensive experience and expertise in information assurance supporting Federal Government contracts, as a Certified Information Systems Security Professional (CISSP) and a Project Management Institute (PMI) Project Management Professional (PMP) to screen and ask appropriate questions that will facilitate the development of a model.

The literature review and interviews provided insight into the risk management issues for information assurance contracts and a problem statement was developed that guided the development of research questions and objectives for the research. The proposal for this research was presented to the dissertation committee with nine research questions, which were scaled back to three questions.

The dissertation committee also recommended that a data collection model with a minimum of ten industry experts be interviewed and their responses be used to answer questions based on the taxonomy developed, as opposed to performing an online survey of 40 plus participants. This was recommended as the preferred method to improve the validity of the research.

Industry experts and academia ascertained the value and possible contributions of this model to the field of information assurance and project management.

1.6 PHASE 2: Taxonomy Model Instrument Development

The researcher then developed an information system breakdowns structure model and an e-Government Relational Technical Control model that consisted of entities and relationships and develop risk mitigation and management strategies for the identification and authentication control family that are base on the NIST SP 800-53 Rev 3. A data collection questionnaire was also developed to assess the components and value of the contribution of the information system breakdowns structure, e-

Government Relational Technical Control Model and the identification and authentication risk mitigation and management strategies for improving the security posture of information systems.

Prior to the use of the data collection questionnaire, the researcher assessed the value of the questionnaire by soliciting feedback from the dissertation committee, select industry representatives and performing a pilot test. Based on the feedback received, the questionnaire was modified to improve its readability, enhance its data collection, clarify some questions and minimize ambiguity. Recommendations and suggestions from industry experts and members of the dissertation committee for improving and validity, structure, content and coherency of the data collection questionnaire and process were incorporated in the final design of the questionnaire.

To ensure the validity of the data collection questionnaire, the researcher identified information security contractors, network engineers/administrator and project managers working on information assurance Federal Government projects, that have a minimum of four years of experience performing security assessments. The questionnaires were emailed to pre-selected respondents because it allowed the respondents the liberty to select the best time to complete the questionnaire. It also allowed the researcher to reach a diverse group of respondents that would have been impossible to reach due to their diverse locations and security clearance requirements. Survey development literature reviewed indicated that this method tends to be the most suitable method to reach the survey respondents.

The gains in the validity and reliability of data obtained by using this method outweigh the possible validity and reliability that may be obtained by selecting respondents from a centralized location (the Washington DC Metropolitan Area) or by using an online survey of respondents. In addition, the respondents had extensive experience working on diverse US Federal Government information assurance projects.

The data for the pilot test of five respondents was collected in Microsoft Word 2007 and 2003 documents for validation of the questionnaire. For the field data collection the questionnaire was emailed to the respondents. The researcher decided against the use of a web-based form to ensure that web-form timeouts do not affect the response rate. The data was transferred to SPSS Version 18 (also called PASW Statistics 18.0) for ease of analyzing and reporting on the data.

1.7 PHASE 3: Field Data Collection, Analysis & Validation

The primary respondents selected for data collection are information security contractors, network engineers/administrators and project managers working on Federal Government information assurance projects that have over four years of experience performing security assessments using the NISTSP 800-53 Security Controls.

The researcher invited the National Institute of Standards and Technology (NIST) Computer Security Department and the International Information Systems Security Certification Consortium $(ISC)^2$ Inc. to participate in the survey development and research process. The International Information Systems Security Certification Consortium $(ISC)^2$ Inc provided access to information security contractors with the industry recognized Certified Information Systems Security Professional credential. The researcher encouraged the National Institute of Standards and Technology to participate in the taxonomy model development, as they are primarily responsible for developing risk mitigation and management strategies for the Federal Government and Federal Government Contractors.

The researcher reviewed the expertise of prospective respondents as they relate to information assurance and project management and selected a group of fifty-five respondents to invite to participate in the data collection exercise. An introductory email was sent to the prospective respondents. It highlighted the purpose of the study, risks, and expected duration to complete the questionnaire and asked if the recipient would be interested in participating in the research. Recipients who

responded in the affirmative were emailed an electronic copy of the UMD Information Assurance Research questionnaire and asked for a date that the researcher could expect to receive the completed questionnaire. The framework for answering the questions was based on fifty percent of the information assurance projects the respondents completed within the last year.

The data collected from the interviews was analyzed using statistical methods that included descriptive statistics, factor analysis, bivariate correlation analysis and Bayesian Probability. The statistical analysis revealed trends in managing information assurance for Federal Government agencies. In addition, a case study was used to validate the research results. The case study was analyzed to identify supported hypothesis, unsupported hypothesis and the reasons for the inconsistencies. Finally, the researcher drew conclusions and discussed the results of the study.

1.8 Expected Outcomes of the Research

The research will provide structure in the following areas of project management for Federal Government information assurance contractors:

- Enumerate the information systems that are typically found on Federal Government information assurance projects.
- Provide an e-Government Relational Technical Controls taxonomy that can be utilized to identify the relationships between information systems, users and the e-Government Technical Security Controls.
- Identify effective risk mitigation and management strategies for the identification and authentication control family
- Develop an identification and authentication control family security assessment cost model.
- Provide a common lingua for information security contractors, network engineers/administrators, project managers and pertinent stakeholders to use in discussing the risk mitigation and management strategies.

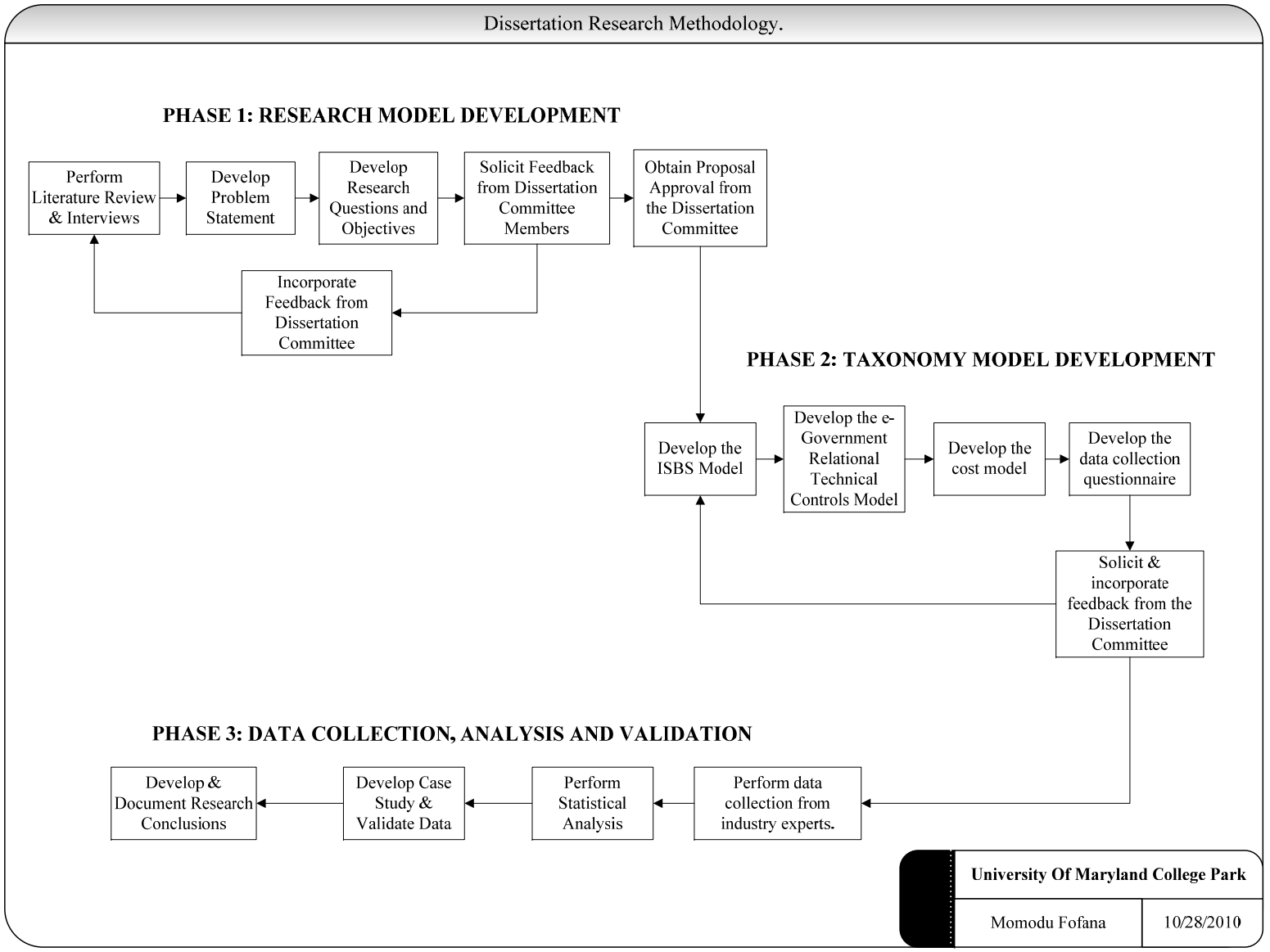

Figure 1.1 Research Methodology

1.9 Application Scenarios for this Research

Information security contractors, network engineers/administrators, project managers and pertinent stakeholders can use the information system breakdown structure (ISBS) model to enumerate projects physical resources during a security assessment.

The e-Government Relational Technical Controls taxonomy can help information security contractors, network engineers/administrators, project managers and pertinent stakeholders develop a framework for discussing information assurance security control entities and their corresponding attributes. The identification and authentication risk management strategies will highlight the NIST risk management strategies that information security contractors believe are effective for managing risks. It will delineate the risks management strategies and their corresponding relationships to users and information systems for information assurance projects. This approach will allow for the effective identification and categorization of information systems risks so a project manager or information security contractor can easily reuse them after identifying those that are applicable to the project and prioritizing their application on a project-by-project basis.

To mitigate the risk to a project without looking at the potential risks to information and assets is to assume that by ignoring those risks, we can prevent their impact on a project. Scientific research has repeatedly shown that tasks that are not monitored and controlled have a higher probability of causing a negative impact on a project. This results in a trend wherein ignored tasks become showstoppers that can derail information assurance projects.

The future of project management lies in its capability to not only mitigate risks associated with project tasks but also to mitigate risks associated with the use of information systems. Information systems are not only a tool to achieve the goals and objectives of the project but also as a major contributor in determining the success or failure of a project and consequently its organization.

The taxonomy framework that will serve the following major objectives:

- Sensitize project managers to risks facing information assurance projects.
- Provide a basis for project managers to develop project management methods for identifying vulnerabilities and managing risks to information assurance projects.
- Allow project managers to develop a fulsome solution for meeting project goals in their project plans and consequently take the mystery out of information assurance projects.
- Improve forecasting of information assurance threats on projects.
- Perform cost/benefit analysis for eliminating information assurance risks.
- Determine to what extent the cost of compliance starts to affect the bottom-line to the organization and, where possible, define a break-even point where the costs of compliance can become a direct project cost that can be passed on to the customer or to a third party in the form of insurance.

Chapter 2: Literature Review

2.0 Information Security for Organizations and Projects

Information technology is an extensive and dynamic industry and is a critical factor in determining the outcome of a project. Information technology when used efficiently helps organizations decrease the time to market and provide solutions for meeting the dynamic requirements of different stakeholders. Information technology helps projects to recognize and implement catalytic responses to changes in the business environment.

Whitman (2008) observes that the role of information technology serving just a centralized group of stakeholders has changed to one where it now serves globally dispersed stakeholders. As a result, the problem of computer security for a small-scale installation has morphed into one of information security for all the systems that support the organization. The result is that the responsibility for information security should not be the onus on the information technology group. It should be the responsibility of employees, managers and other stakeholders involved in the business of the organization. A fitting question to pose is "how can research help in reducing the knowledge gap between information security experts and key stakeholders within organizations and projects?"

Whitman et al (2008) provide a general definition of security as the quality or state of being secure: to be free from danger. To be secure is to be protected from adversaries or other hazards. He maintains that information security must be properly planned, organized, staffed, directed and controlled. His stance on information security being properly planned, organized, staffed, directed and controlled in an organization alludes to the fact that information security is a good candidate for project management methodologies. In addition, the dynamic and evolving characteristic of information security lends itself to the project management framework wherein an

iteration of the five-project management process facilitates information security processes.

2.1 IA Government Contractors Organizational Structure

The Project Management Body of Knowledge recognizes the following organizational structures as the typical configuration of most organization:

- Projectized Organizational Structure
- Composite Organizational Structure
- Balanced Matrix Organizational Structure
- Strong Matrix Organizational Structure
- Weak Matrix Organizational Structure
- Functional Organizational Structure

The configuration of the organization structure for information security departments of Federal Government contractors depend on the perception of upper management on the services delivered by the information security program. This typically dictates the existence of a Chief Information Security Officer (CISO), their authority, resource availability, budget control responsibility and administrative staff availability to support the departments or project goals and objective. The organizational structures listed above have their inherent advantages and disadvantages, which directly affects the delivery of Information Assurance services to Federal Agencies. These advantages and disadvantages are discussed in the current PMBOK guide and are not elaborated in this research.

Whitman (2008) recognizes that an organization's size and available resources directly affects the size and structure of the information security program. Organizations with complex IT infrastructure and sophisticated users usually require more information security support than those that are smaller and have less complex users. The general rule of thumb is that the larger the organization, the larger is the

information security program. For smaller organizations, it is common to find an entire organization supported by a single security administrator. Smaller organizations tend to relegate the duties of the security administrator to the network or systems administrator.

The article "Does Size Matter" by Briney (2002) has the following to say about the size of the information security program in reference to the size of the organization "*as organization get larger in size, their security departments are not keeping up with the demands of increasing complex organization infrastructures. Security spending per user and per machine declines exponentially as organizations grow, leaving most handcuffed when it comes to implementing effective security procedures.*"

The position proposed by Briney (2002) has changed because of multiple reported information security breaches that have resulted in negative publicity, loss of jobs, market share and extensive fines imputed to negligent organizations. Information security is viewed as a critical function for the existence of an organization. Even though the change process is already in place, its pace is restricted by economic limitations plaguing the US economy. Table 2.1 shows a synthesis of the results of the research conducted by Briney (2002) showing how the size of the organization and its corresponding expenditure on its information security program. Information discussions with information security contractors indicated that not much has changed since 2002 except that the programs now have to do extensive documentation, which in most cases does not improve the security posture of the organizations.

The size of the organization typically influences the configuration of the information security program yet every organization should be capable of performing certain basic business functions. Whitman (2008) maintains that all organizations should be capable of performing the following security business functions:

- Risk assessments and management
- Systems testing

- Policy and Procedures development
- Legal assessment
- Incident response
- Planning
- Measurement
- Compliance
- Centralized authentication
- Systems security administration
- Training
- Network security administration
- Vulnerability assessment

Table 2.1 the Information Security Budget Percentages for Different Organizations

Size	Computers	IS Management	IS Budget	Comments
Small	10 – 100	Centralized – usually assigned to one person who handles administrator, network and security issues.	20% of the IT Budget	• Usually one person • Spend more per user than medium and large-sized organizations • More than two-thirds of these organizations say all/most of their security decisions are guided by management-approved policies • 57% said that all or most of their responses are guided by a predefined IR plan • Does not have a CISO. May have one full-time individual assigned to security and possibly a part-time support staff member
Medium	100 – 1000	Security staff usually relies on IT staff to assist with implementing security plans and practices.	11% of the IT Budget	• Their ability to set policy, handle incidents in a regular manner and effectively allocate resources is worse than any other group • For their size, the number of security incidents recognized is skyrocketing • Seventy percent of them had damages that were imposed from security breaches. This was 48% higher than for small organizations • May or may not have a CISO, but usually has one full-time individual assigned to security with three part-time individuals supporting the information security effort
Large	1000 – 10,000	Usually has a decentralized security program for the different projects within the organization.	5% of the IT Budget	• Generally have integrated planning and policy within their organizational culture. Eight of ten organizations claim that their security decisions are guided by their policy and plans. • Information security approaches appear to be as diverse as the organizations. • Has a CISO, 1-2 full-time administrators, 3-4 full-time administrators/technicians and as many as 16 part-time staff members who have security duties in addition to duties in other areas.
Very Large	>10,000	Usually have an internal dedicated entity that deals with information challenges for the organization	6% of the IT Budget	• Large information security budgets that grow faster than their information technology budgets. • Due to the economies of scale, very large organizations tend to do a better job on policy and resource management. • About only a third of these organizations handled incidents according to their incident response plan • These organizations are usually staffed and funded at a level where they can effectively manage information security. • May have multiple CISOs that are responsible for the security of the different branches of the organization. May have more than 20 full-time security personnel and 40 or more individuals with part-time responsibilities.

2.2 Information Security Management vs General Management

Whitman (2008) observes that as the Internet continues to grow, the interconnections between networks become vital to the smooth operation of commerce. Organizational reliance on information systems has increased over the years and there has been a corresponding increase in the number of incidents of information security breach. The increasing attacks on information systems and the success of criminal attacks indicate there is a need for increased information security. We must mitigate and manage these risks as their potential to disrupt organizational operations, change organizational equity and precipitate organizational structure changes in the chief cadre makes them critical.

Project managers must be proficient in recognizing the threats and vulnerabilities associated with the use of information systems and strive to become efficient at managing information security risks that are associated with the design, development and use of information systems. They need to identify repeatable project management strategies that can address the threats posed by organizational information systems. Whitman (2008) also propose that the management of information systems is a management problem and not one that technology alone can answer, as the problem has important economic consequences for which management is accountable.

Whitman (2008) maintains, “There is a general trend for management not to take information security seriously. This may be in part because information security is still a relatively new field and there are still lots of gray areas. It may also be because generally management doesn't have enough knowledge or care to be educated about information systems technology.” Information security usually finds itself competing with known and proven objectives like lowering cost, return of investment, increasing speed, increasing user-friendliness, reducing time to market of new products etc. Information security has a tough time winning against these proven methodologies and we are not trying to make a case that information security should win. We are suggesting that the parties should work toward a fair ground wherein information security and general management achieve a win-win scenario based on some

weighted decision analysis that integrates management concerns with those of information security.

Information security is very dynamic and top management has not been able to appreciate the changes taking place within information security. The destruction of the Enron and Arthur Andersen documents by Arthur Andersen can be seen as a case wherein information security failed. In as much as the destruction of information technology documents are a part of the information life cycle. The management of the destruction of documents must follow specific statutory, organizational and business policies in a controlled manner for it to be acceptable in the information security field. We can say that the lack of training or proper practice of information security contributed to the downfall of one of the world's finest accounting firms. We need to move information security to a position wherein top management can appreciate its contribution to the organizational goals.

There is a general trend for the public not to believe in the government or businesses in the handling of their private information. This may be because news media is rife with cases wherein either government data is stolen or some organization loses its laptops, hard drives or tapes in transit. Whitman (2008) stresses that “There is a general belief in information technology security that the adoption rate of electronic transactions will more than double if business and the government can convince consumers that their private information will be adequately safeguarded.”

With all these scenarios, top management still does not appear to appreciate the importance of information security or its role as a competitive advantage. The ability to be able to double sales should be very important to management yet we observe that information security suffers from insufficient resource allocation. Most organizations do not have an established Chief Privacy Officer. Whitman (2008) proposes that “Top management doesn't appreciate how doing a good job in the information security realm will lead to a variety of tangible business benefits” like more business referrals from content customers.

Job descriptions, department mission statement and outsourcing contracts should reflect an organization's position on information security. Yet we see several organizational cases where this is not the case. In the assessment of Federal Government contracts, a review of the rating assigned for including security in job descriptions, department mission statements and possible outsourcing contracts will provide some insight into the importance of security to organizations. Some typical examples would include security for personal computers that specifies that all personal computers must have virus detection software that performs daily updates, hard drive that is encrypted and must be unlocked before the operating system loads, personal firewall that performs port and application filtering, email filters and other related security software. In addition, users need training on how information security and social engineering affects their computer, the projects they work on, the organization and their business partners.

Sometimes when we refer to users, we fail to identify the unforeseen stakeholders like the janitors that have an equally important stake in information security for in most cases they are the primary building custodians and have access to the entire building. For most small organizations, the storage closet of the janitors also doubles as switch storage that has data flowing through, thus the importance of having security training at all levels of the organization cannot be underestimated.

All stakeholders with access to sensitive, valuable or critical information must receive information security sensitivity training. The number of stakeholders has increased not only with E-Commerce but also with the identification of new ways to hack systems. Janitors for example must know that they should not allow personnel they know to piggyback on their physical access rights. They may have been terminated earlier in the day and are trying to gain access to restricted locations. Their training should include sensitizing them to the effects of moisture and chemicals on information systems equipment like switches, routers etc that may be housed in the closets.

The question that comes to mind is “Do current Federal Government contracts for cleaning services require proper security screening and due diligence training for all personnel?” We know that a security infrastructure is only as strong as its weakest link. Is it possible that this is one of the weakest links in Federal Government Contracts? Given that a network or security environment is only as strong as the weakest link, we need to do more in security training to ensure that assets are secure. There is also a need for training on how to handle confidential information. What information can or cannot be divulge to outsiders? How much of these tasks should be the responsibility of the project risk manager and if so is it supposed to be a one-person role? No component in the NIST security controls addresses cleaning staff. This research cannot address all these questions but they are good issues and concerns that should be elucidated for future research.

Organizations must encourage their stakeholders to question, understand and approach security from a holistic approach and put in place blanket policies of security that apply to all stakeholders and specialized security policies for entities and individuals based on their security access level and their need-to-know. An entity’s need-to-now is one of the primary metrics for granting access to information. When will organizations commence the development of an implementation strategy for ensuring need-to-know compliance for applications and information systems? When we start to assess the facets that needs to be coalesce to build a fully integrated security program. It is clear that the approach needs to be relational, customizable and nimble to meet the ever-changing security needs of organizations. The current hierarchical approach would not suffice.

Organizations also need to establish policies for security incidence escalation. Project managers need to understand the Federal Government contractual requirements for incidence response and escalation. These policies should specify what an entity or individual needs to do when they identify/observe a security breach. The policy should also dictate how the breach is to be addressed. What metrics are in place to measure the effectiveness of the incidence response and

escalation policy and procedures? What factors of these metrics lie on the critical path of the implementation and what is the best method for controlling them? Whitman (2008) maintains that the first step in resolving an organization's security posture is to identify the weaknesses. How can we begin to resolve the weaknesses if we are failing in the threat identification process? Would the e-Government Relational Technical Control taxonomy for information systems improve our ability to identify project and organizational threats? What are some of the project management challenges facing the identification process? Will a study of our current incidence response techniques help us improve our information systems risk management methods?

2.3 Characteristics of Organization Risks

Abkowitz M. D. (2008) studied well-publicized potentially preventable cases that include natural disasters, man-made accidents and terrorist acts that either occurred in the US or abroad. Some of the cases studied include the Hyatt Regency Walkway Collapse, Attack on USS Cole, September 11: The World Trade Center and United Airlines Flight 232. He studied the cases under ten risk factors that contributed and consequently resulted in either disastrous or mitigated events. His study included the causes, impact and ripple effects of the events. From the study of the cases, he developed a summary of lessons learned and provided a summary of risk characteristics typical in the cases studied.

A summary of the Abkowitz research findings include the following:

1. We need to develop a methodology for decoupling risk factors
2. We need to ensure efficient communications between all stakeholders
3. We need to do a better job at project planning and risk management
4. There is a need for us to pay attention to details when dealing with man-made projects.
5. We need to ensure we have sufficient resources assigned to projects and be aware of how political agendas or personal biases might affect our judgment and those of other stakeholders.

6. We need to institute and ensure utilization of standard operating procedures as far as possible while ensuring that we have a contingency plan for undesirable events.
7. We should utilize probability to estimate risks that may affect projects and be willing to acknowledge that even with the best of our efforts, 'to err is human'.

Abkowitz (2009) proposed that the goal should be one that is to be oriented towards becoming an organized master of risk management instead of becoming a victim of risk and accepting the fact that unfortunate events will sometimes occur no matter how well we plan. The products of this research will address all aspects of Abkowitz's recommendations.

A study by Bazaz (2007) also found that factors contributing to the vulnerability of software applications include: the complexity of the application because of its size in reference to lines of code and multiple services provided by other applications, the number of potential vulnerabilities and the complexity of the vulnerabilities. He also noted that some of the vulnerabilities "involve multiple software components interacting to produce a vulnerable system state." These factors combine to increase the level of complexity of the vulnerabilities associated with applications. Can we develop some form of artificial intelligence that can help with decision-making for information security and if so, what are some of the risks associated with using such a tool and how can we mitigate and manage them to acceptable levels?

Tom Davis, Chairman of the Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina Hearing on Preparedness and Response in Louisiana, questioned the Governor of Louisiana, the Louisiana Office of Homeland Security and Emergency Preparedness, the Mayor of New Orleans, the Mayor's Director of Homeland Security, and the Federal Emergency Management Agency (FEMA), in an attempt to understand the success and failure to the challenges posed by Hurricane Katrina of August 25, 2005. His questions include:

were federal, state, and local governments coordinating their response effectively? Who was responsible for getting people food, water, and medical assistance while they waited? How much did telecommunications problems impede effective response? It is common knowledge that one of the major problems between first responders was that communication devices were communicating on different frequencies so relief efforts could not be effectively coordinated. How much of the compounding problems of this disaster was a result of the inefficient use of information systems?

Again, we see the request for an assessment of our incidence response efforts that attempts to see how telecommunications challenges, among other factors, may have compounded the problem. How effective would Abkowitz's suggestion of decoupling the risk factors contributed to alleviating some of the problems experienced during the aftermath of the hurricane? Did the inability to effectively storyboard or test risk mitigation and management plans contribute to us becoming a victim to risk?

Per Charette (1989) risk can be categorized into the following three categories:

- Known risks: These risks can be identified by careful review of the project plan and the environment in which the project is developed
- Predictable risks: These risks can be identified from experiences with similar projects.
- Unpredictable risks: These risks are hard or impossible to predict.

Not ignoring the fourth category recently introduced by Dick Chaney as the unknown unknowns. How well can we use Charette's model to decompose the risks encountered in information systems and will it help us understand the information assurance risks? Of those that are known and predictable, what have we done to mitigate and manage them in our communities?

2.4 Information Assurance

Information assurance is a dynamic industry and the trend is that new technologies for information assurance are always playing catch-up with hackers. Perrow (2007) alerts us to the fact that several Department of Defense (DOD) computers were hacked in February 1998. The culprits were able to obtain 'root access' to the computer, which could allow them to alter or steal information on the computers or damage the DOD network. The attacks went on for a month and were initially believed to be a case of 'information warfare' by the Iraqi Government but computer forensics later tracked the attacks back to two California teenagers assisted by an Israeli teenager. This was the state of Internet security in 1998 and much has not changed since.

We have historic records of several incidents wherein hackers obtained unauthorized access to nuclear plants, power stations, financial institutions, intelligence agencies as well as the DOD. Perrow (2007) argues that the Internet presents the largest target for fraud and terrorism. This is because terrorists can exploit flaws in operating systems, computers, software and firmware that control our critical infrastructure, to launch information warfare on the US. Terrorists could also obtain access to read, modify or destroy plans of the Department of Homeland Security and DOD, especially since most of these plans reside on information systems.

The vulnerability of our critical infrastructure is well publicized but we have no proof of whether these vulnerabilities have been exploited or compromised. Most of the US critical infrastructure runs on a Microsoft Windows platform, known for its bugs and unceremonious crashes. Yet no method has been developed that can accurately measure how much risk the US critical infrastructure is exposed to due to a concentration of technologies. In addition, no repeatable project management processes have been developed to mitigate and mange the risks posed to the US critical infrastructure.

The article titled "Inside the Chinese Hack Attack", published in the Time Magazine dated August 25, 2005 by Nathan Thornburgh, provides additional evidence of the vulnerability of the US critical infrastructure. Thornburgh affirms that the hackers breaking into official US networks were not only using Chinese systems to launch their attack but they are based in China. The systems hacked during this period include: The US Army Information Systems Engineering Command at Fort Huachuca, Arizona, computers at the military's Defense Information Systems Agency in Arlington, Virginia, the Defense Department of the Naval Ocean Systems Center at San Diego, California and the United States Army Space and Strategic Defense installation in Huntsville, Alabama.

The US Government still does not know what information was compromised or the full impact of the attack on unclassified systems that store sensitive information and provide logistics support to the armed forces. Government analysts that worked on this case believe these attacks are ongoing with increased frequency but we have no knowledge of the purpose of the attacks. This problem is not peculiar to the United States alone.

In 2007, hackers believed to be residing in Russia attacked Estonia with a series of denial of services attacks as reported by the BBC News article of May 17, 2007. The attacks lasted for three weeks during which government websites, banks, newspapers, and several institutions were compromised. The NATO spokesperson, Mr. James Appathurai, in a conversation with the BBC reporter, stated that NATO sent experts to help Estonia defend its organizations. Russia also has a history of attacking the US and Ukraine.

A March 2005 Government Accountability Office report stated that security contractors within the electric industry reported that hackers were targeting the US electric power grid and had actually gained access to US utilities electronic control systems with limited repercussions on the affected systems. We know from an FBI

report entitled ‘Internet Security Review’ of December 2005, that an Internet worm almost shut down FBI Internet access.

A coalition of Chinese hackers successfully launched a denial of service attack on the CIA and White House websites, in response to the collision of a US surveillance aircraft and Chinese fighter jet in 2001. Yet no one could say with certainty what the security breach cost the US government or its impact on our operations. The question research needs to answer is: when will we develop a system or method that we could use to measure the impact of a security breach to our critical infrastructure? Only then can we actually begin to assess and effectively manage the risks therein.

Some other questions we may want to address include: what systems can we run in manual mode without computer interaction? Have the fail-safe modes of the different systems that make up the US Critical Infrastructure been defined and tested? What percentage of these systems can self-correct? What is their self-correct time-line? What is the criticality of these systems and are they suitable for self-correcting applications? What percentage of the vulnerabilities associated with the Internet are a result of a concentration of technology?

A recent 2008 global survey by the PMI Market Research Department that was published in the PM network of May 2009, found that thirty-nine percent of respondents worked in an Information Technology Function with fifty percent of the respondents claiming that their projects utilized virtual teams. With the increasing use of virtual teams, we need to understand how introducing new technologies affects our risk profile and changes the dynamics at play as it relates to managing risks to our critical infrastructure. The information security industry is rife with war stories wherein video conferencing equipment is configured to be in promiscuous mode (always listening) to accept incoming calls. How many closed-door meetings are actually bugged because of poorly programmed video conferencing equipment?

To provide a holistic solution in an attempt to protect the US critical infrastructure, stakeholders need to make decisions among alternative courses of actions. Information security decisions usually involve multiple interrelated factors. A study by Frank (2008) notes, “complicated situations usually involve more difficult decisions and many interrelated factors to consider.” Hammond (1999) showed that "The only way to raise the odds of making good decision is to learn to use good decision-making processes". Frank (2008) also highlights the fact that not all good decisions require the maximum safety solutions as this may make the solution cost-prohibitive or drastically increase the time to market. Probabilistic risk assessment can be effectively used to provide quantitative methods for analyzing risks.

Frank (2008) recognizes a complicated system as one that is difficult to analyze or understand, and that may have multiple interrelated factors or numerous internal and/or external interdependencies for which we do not understand how changes in one of the system variables affect the overall system. For example, increasing the level of safety can coincide with increase in overall cost and decreased product reliability.

This is an organizational research problem that is similar to our experience with project management tools wherein an appreciable delay of a task that was not on the critical path can cause undesired effects in the project plan, like creating multiple critical paths or changing the critical path of the project plan. We need to find ways to identify these changes in real-time and account for them when performing probabilistic risk analysis for projects.

The process of choosing between multiple alternatives also provides the advantage, in that it increases the decision maker’s understanding of the interrelationships of the attributes and alternatives of the system. It may also present unknown opportunities that can positively influence our risk profile or improve our risk management strategies.

Frank (2008) notes that 'the time involved in the process of making potentially dangerous and expensive systems safer needs to be addressed to see how we can control the shortening of the time while managing the risks posed.' Information systems risk management can benefit from the process of controlling competing variables to ensure the safety of our systems and consequently ensuring we can meet our targeted return of investment on projects.

Risk management has heavily affected the information technology profession. Simpson (2008) in his book on Managing Project Risk Best Practices for Architects and Related Professionals claims that 'only in the last 30 years have we had to worry about risks. It all began about the time the request for information (RFI) appeared on the scene.' The result is that we are observing a large increase in the number of claims against insurance companies and litigations among the parties. This increase in claims against insurance companies has threatened the existence of many insurance providers, and premiums and deductibles have risen as they attempt to compensate for the risks associated with the projects while trying to keep their organizational bids competitive.

Most insurance companies and in-house lawyers are recommending risk management strategies and are warning against projects of higher risk. Thus if we don't address the issue of information system risk management on projects, we might experience a situation wherein it will be next to impossible to purchase insurance coverage for these projects and still break even. In addition, Bonham (2008) states it more judiciously succinct that "business continuity insurance can be complex and lead to scenarios in which those who thought they would get compensated don't."

A study by Besner & Hobbs (2006) on various project management tools and techniques showed that of the seventy techniques assessed, risk tools ranked very low in everyday use. The order of usage was identified as follows: risk management documents, ranking of risks, graphic presentation of risk information and databases

of risks. The paper also identified risk tools as being the least exploited area for increasing project performance. They can easily be one of the areas that can generate the highest return for project performance measures. The question that comes to mind is "How can we improve the low adoption rate of risk management tools?" Can the e-Government Relational Technical Controls taxonomy increase the awareness of information assurance based risks on projects?

2.5 Project Management vs. Information Assurance

Jen (2009) maintains that "Poor risk management usually results in a higher probability for project failure". Jen (2009) also highlights the need for "better and simpler risk management to ensure higher adoption rates and continuous utilization throughout the project, thereby increasing the chances for project success." It is insufficient for project managers to understand project management technologies like project risk management; they must also understand how to apply them to information assurance projects and the impact of unmitigated information system risks to the success of projects.

Shore's (2008) paper on "Systematic Biases and Culture in Project Failures" underscores the likelihood of engineering problems having less visibility when compared to project schedules and budgets. Thus, the more project managers become efficient at understanding the engineering problems and risks, the less likely they are to make decision based on selective perceptions. Project Managers need to understand the information system threats and vulnerabilities most likely to impact the project schedule, quality and budget and start identifying risk management strategies for them.

A May 2008 online survey of 7,079 security and IT professionals in 100 countries by PricewaterhouseCoopers showed that 59% of the companies reported having an overall information security strategy. It is a common belief the greatest threats to a project's security is from hackers and other external menaces.

Wheatley M. (2009) paper title 'an inside job' alludes to the fact that "security breaches are shown to be 'inside jobs,' rather than machines or ill-intended humans breaking in." He maintains that the project teams are the true threat to projects because of human error, laziness or negligence. He also provides convincing evidence that the organization's security policy should suffice except in cases where in the project calls for tighter controls. The one-size-fits-all approach for risk management is unsuitable for project risk management, as the risk management policy should be streamlined with the statutory, stakeholder expectations and organizational requirements of the project.

When a project manager observes something untoward, they should not assume that the security team would show up and take care of things. Project managers should take a proactive approach to addressing security requirements and ensure that security vulnerabilities that may affect the project are mitigated to levels where they may have little or no effect on the project schedule, customer satisfaction, cost and quality.

What project assets do organizations need to secure? Wheatley (2009) proposed, "Everything connected to a project should be secure – not just data that might be used as part of the development or testing processes." Some of the entities that his paper recommends protecting include the following: the privacy of source documents, planning documents, team communications, test strategies algorithms and knowledge. Protection of assets should not be limited to personally identifiable data like credit card numbers, social security numbers, driver's licenses and medical records. Wheatley M (2009) observes that, "too often, companies don't build security into their IT project plan and as such it is usually tacked on as an afterthought." He also maintains that making a project secure does not have to be expensive or complicated. This research cannot attempt to address all the domains highlighted by Wheatley (2009) that needs to be secure within organizations. It shall only address issues raised in the research questions.

Whitman (2005) described information security in terms of confidentiality, integrity, availability, privacy, identification, authorization and accountability of information. We acknowledge that information security involves more than just the technical solution.

The US Federal Government enacted a Federal Information Security Management Act (FISMA) of 2002 also called the E-Government Act that requires all Federal Agencies and contractors establish and maintain certain security controls for assessing the security of their information systems. Whitman & Mattord (2005) states that 'the US has not established any mandatory standard.' Yet in the information security circles, the fight is on between the government and industry of whether to regulate or not to regulate. Currently, it is a requirement for all Federal Agencies and Federal Government Contractors to meet the FISMA requirements. Organizations that want to remain competitive while adhering to regulations would be well advised to plan accordingly.

Organizations rely on a combination of security guidelines from NIST (like the Special Publication 800 series documents), ISO 17799 and other industry consortiums. Other information security standards include: Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley, the California Database Security Breach Act (Certification and Accreditation SB 1386). The general rule of thumb in deciding what information security standard to follow is that the standard should align with the organizational objectives. How does this apply to projects that may span multiple locations or incorporate multiple domains? If we are developing an application for a health care facility, what amount of reciprocity exits between the HIPAA and the NIST standards? Suppose our project spans multiple countries including the UK and the US. What standard takes precedence? What role does jurisdiction play in the selection of the appropriate standard to implement? How much do we need to invest on documentation and security assessment of information security program to show due diligence in the case of a security breach? We cannot even begin to assess how insurance factors into all this.

D'Arcy (2009) maintains that most of the current research on standards for information security management is limited to critical analyses of these standards, prescriptive advice on standard implementation and assessments of standard compliance. Very little research has been performed on assessing the post implementation effectiveness of many of these standards. As a result, we have no measure of the effectiveness of these standards, to reduce number of security breaches. This research shall address this concern by looking at the NIST SP 800-53 Rev 3 security assessment strategy for the identification and authentication control family. What are the effects of the industry, culture, size or geopolitical differences in the effectiveness of these standards?

Tejay (2005) maintains that it is not feasible to adopt every standard or every single facet of a particular standard. Thus, we need to study the effectiveness of the different standards in the different organizational contexts. This will provide managers with effective implementation guidelines for the different standards vis-à-vis their organizational profile. For this research, we are assessing the NIST SP 800-53 Rev 3 against Federal Government Information Assurance Contractor organizations.

D'Arcy (2009) maintains that some regulations have been developed that require organizations that do business with the public to abide by these standards, yet there is very little research on the impact of these standards on organizational security policies and practices. How do these regulations affect multinational organizations that span several countries? Hovav (2005) maintains that the costs associated with meeting regulatory compliance could become prohibitive and the cost for non-compliance can be substantial. What are substantial non-compliance costs?

The Federal Trade Commission Report of January 26 2006 notes that ChoicePoint, a consumer data broker, was ordered to pay $10 Million in Civil Penalties and $5 Million for Consumer redress after they acknowledged that personal financial records of more than 163,000 consumers in its database had been compromised. "FTC

charged that ChoicePoint violated the Fair Credit Reporting Act (FCRA) by furnishing consumer reports – credit histories – to subscribers who did not have a permissible purpose to obtain them, and by failing to maintain reasonable procedures to verify both their identities and how they intended to use the information." ChoicePoint security and record-handling procedures violated consumers' privacy rights and federal laws. The settlement called for annual audits by an independent third-party security professional every year until 2026, the establishment and maintenance of a comprehensive information security program and a cease and desists of their current data sharing practices.

A recent case of data breach by three HSBC firms happened in the UK and reported on the Financial Authority Services (FSA) web site on July 22, 2009. The opening statement to the publication at the website read as follows, "The Financial Services Authority (FSA) has fined three HSBC firms over £3 million (approximately $4.7 million) for not having adequate systems and controls in place to protect their customers' confidential details from being lost or stolen. These failings contributed to customer data being lost in the post on two occasions."

www.pillsburylaw.com published a statement on July 1, 2009 surrounding the settlement arrived at on June 23, 2009 between TJX (commonly known as TJ Maxx) and forty-one state Attorneys for the sum of $9.75 million. The lawsuit arose from a security breach that occurred in 2006 that affected millions of credit card customers. This lawsuit also creates a precedence where in states are beginning to look to future security breaches as a sustainable source of funds.

2.6 Project Risk Management

One of the primary goals in managing projects is to meet or exceed the customer's expectations while managing cost, time and quality. It is a common belief in the field of project management that exchange of ideas is the best way to mitigate risks on projects. How do we begin to communicate with the customer and pertinent stakeholders to ensure we are all on the same page when it comes to risk management

without agreeing on taxonomy of common terms? Let us not forget that “conflict thrives in confusing situations”.

A research paper by Susan Ladika (2009) on “The Incredible Shrinking Team” identifies that a major advantage of lean teams is that “it’s easier to communicate with five or six people versus 50 or 60.” Also with the current market dynamics, we see a trend towards leaner teams that are more efficient and tend to benefit better from enhanced communication because of their smaller size.

Even as teams become smaller and have the advantage of being nimble, there is a need for them to ensure that they are communicating on the same terms and understand the client requirements so that their deliverables meets the expectations of the customer. The need for extensive teams of support staff to support smaller teams is reduced. Teams in the construction industry cannot be this small because of the diverse nature and they are very dynamic because of the ever-changing team configurations. These team have a need to effectively communicate and mitigate risks to the projects. The use of information systems to facilitate communications also introduces a different set of risks to a project.

It is a generally accepted fact that a project has a better chance of being successful if it develops and utilizes a taxonomy that specifies the terms of the contract even before a contract is signed. This will provide the stakeholders with common, accepted terms that could help not only with communication but also in the development of design requirements instead of waiting for the design phase to address problems for improperly defined terms, which usually results in scope creep, change requests, increased costs and reduced customer satisfaction. In addition, the costs associated with errors made during the development of taxonomy at the planning phase are usually much lower than the costs associated with a product redesign due to misunderstood requirements. We must note that even with the best contract vehicles there is always some latent risk borne by the contractor and the project sponsor. Therefore, it benefits all parties to explore the use of taxonomies.

I propose that the e-Government Relational Technical Security Controls taxonomy be reviewed prior to the contract award as by the time the project reaches the communications-planning phase, the contract is already awarded and the likelihood for scope creep increases. The only way it is possible to utilize the e-Government Relational Technical Security Controls taxonomy when responding to requests for information is if one already exits that can be adapted or customized to the project needs and used for proposal development to identify the scope of work.

According to both the S and J curves for the life cycle costs of projects, we know that it is always cheaper to make changes to a project design before costs are committed as opposed to attempting to make changes in the final design of the product. Trying to incorporate changes in the test phase as add-ons, inevitable service patches and upgrades has resulted in the birth of the term "software assurance", which has a tendency to increase the total cost of ownership. We must not forget the losses due to the opportunity costs in the time spent developing service patches for an application, as well as the opportunity cost and missing the opportunity to seize first mover advantage if we choose not to develop the e-Government Relational Technical Security Controls taxonomy.

Jen (2009) states that 'Due to "higher" priorities, project managers do not wish to spend time on non-value-added activities, which is unfortunately how they often view risk management'. We need to facilitate a culture change towards risk management through education of project managers on the importance of managing information system risk. Unless we can educate our primary stakeholders on the importance of risk by helping them identify the potential threats to the successful completion of the project, we cannot expect much change in the attitudes of project managers towards information system risk management.

For that education to begin, we need to set the stage for speaking about information security risk management at the project level by developing this e-Government Relational Technical Control taxonomy that will facilitate the discussion.

2.7 Project Risk Manager

The role of the project manager is not limited to managing the project but also, as Keyes (2009) states, "The PM must thoroughly understand the various risks that may affect the implementation and must be prepared to manage them. Risks may be internal or external." Keyes identified internal risks as risks that the project team can manage, such as staff assignment and cost estimates while external risks are beyond the control or influence of the project team. External risks include market shifts or failure by outside vendors to perform.

The project manager must be capable of developing a risk management plan as part of the project plan that includes information security aspects that can derail a project. They must also be able to quantify and assess the impact of the risk identified to the successful completion of the project. Jen's (2009) paper, Visual Ishikawa Risk Technique (VIRT) – An approach to Risk Management, has the following to say on how PMBOK addresses risk management "Other than Quality Management, Risk Management is likely the most misused and underutilized knowledge area of A Guide to the Project Management Body of Knowledge."

Most project managers work in environments that utilize Information Systems to facilitate the accomplishment of the project goals. Information Systems can be a double-edge sword that can be the project manager's best servant or their worst nightmare and may contribute to the high failure rate of projects. Prior discussions in this paper have shown how threats in an application or operating systems may pose risk to the project and the viability of the organization. A typical example will be the case wherein a project server that is used for responding to requests for proposals experiences a security breach resulting in the loss of proprietary information,

intellectual property or, worse still, information ending up in the hands of the competition and a possible consequence of continued failed bids.

Organizations may have the best caliber of employees using current project management methodologies and tools but if they are vulnerable to attack then by Moss's law and the law of probability [Pr (event) = $e^{-\lambda t}$], given sufficient time, they will experience a security breach. If they are always vulnerable to attack because they are not utilizing information assurance best practices the λ value increase and this consequently increases the likelihood of an information assurance risk derailing a project.

Organizations may find that they not only lose face in the eyes of the public but their insurance may refuse to compensate their loss if they can prove that the organization was negligent or did not use due diligence to mitigate their potential losses. Organizations that do business with the Federal Government have to abide by strict regulations, with penalties for negligence being in the millions, as was the case with ChoicePoint. No value can be place on the intrinsic loss of 'good face' organizations may experience with their stakeholders.

Project risks are not limited to information assurance risks. They may also involve organization risk, environment risk, business risk, product risk, employee risk, etc. Project managers need to identify ways for ensuring that when executing joint ventures with external organizational entities, their partners can only see information necessary for performance of the project and within the scope of the joint venture. They must also be able to discuss potential exploits in software or code that might expose classified information to entities that should not have access to them.

A takeaway is that in as much as it is important that we track items on the critical path of the project and utilize earned value management to track and control cost and schedule of a project. We must also be sensitive to the need for us to understand and track the threats and vulnerabilities posed by the systems used to accomplish the

project. This scenario creates a need for project managers to have an understanding of the rudimentary terms of information assurance. Historically, the best way to approach new topics is with taxonomy development.

With the dynamic nature of information security, the question then becomes "Can we begin to develop information assurance taxonomy for assessing information systems based project risk?" The stakes are high and we cannot become overwhelmed by the fact that information systems threats and risks are a moving target and thus any effort to identify processes for managing information systems based project risks are futile.

2.8 Information Assurance Risk Management

Information Assurance is defined by the National Security Agency as "The set of measures intended to protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality and non-repudiation." The goal of information assurance is to assure the quality of information, which inspires confidence in the use of information by its stakeholders. Whitman (2005) describes information security in terms of the confidentiality, integrity, availability, privacy, identification, authentication, authorization and accountability of information.

Research in risk management started in the computer science field and as a result, it has been largely influence by computer science research. One of the earliest researches in computer security started with a security matrix that allowed developers to specify the access controls for users of a system (Conway et al 1972). Bell and LaPaudula (1976) established a method for segmenting of processes into different memory segments and rings to prevent memory over-write or access elevation. Then in the eighties' the US National Security Agency produced a series of security documents called The Rainbow Series. These documents included specifications for secure computer designs that helped stakeholders meet the US Department of Defense's criteria for trusted computing.

Bonham (2008) has the following to say about the current risk landscape, “no risk initiatives have shocked corporations into adopting operational risk management procedures more thoroughly than the recent passage of such government regulations as Sarbanes-Oxley, Basel III, the Health Insurance Portability and Accountability Act, and Gramm-Leach-Bliley.”

Some risk assessment models that deal with specific assessment of risk within a risk scenario include the Risk Level Matrix, Business Impact Analysis and the Annualized Loss Exposure (ALE) (Krutz 2001; Stonebumer 2002; Tipton 2000). Ng. R (2009) maintains, “The ISO 17799 “common information security architecture” and Zachman’s information system architecture provide an enterprise level and a comprehensive approach to enterprise risk management.

Currently, the National Institute of Standards and Technology (NIST) develops documentation called the NIST Special Publication 800 series that specifies best practices for secure information design, implementation and management in an enterprise environment. Several researches on risk analysis methods suggest that the security of information systems improved if we incorporate security controls in the system life cycle design. A concern posed by Baskerville (1993) to this approach is whether we can efficiently assess a different set of information systems using controls developed from another type of information system. This e-Government Relational Technical Control taxonomy will address a subset of Baskerville’s concern, by ensuring that the controls are partitioned for the different types of information systems in the enterprise.

Park (2009) states that “It will be difficult for any technology or security mechanism to ever be created that will completely secure the risks of the commerce application.” Information security professionals and entities involved with e-commerce will always be on the defense and developers need to be nimble in developing applications that address threats in applications. Park (2009) also alerts us to the fact that society must have a reasonable grasp of what technology is and where it is going as technology

and e-commerce greatly influence the way we live, work and play. He also draws attention to the need for legislators to be aware of the issues surrounding technology so they know what laws to legislate.

Most of the tools available for risk identification, assessment, mitigation, transferring, monitoring and control require ongoing communication between the different stakeholders. Excessive communications between information security contractors and project sponsors on the finer distinctions of the terms of the contract often become an impasse to a project's success. The information systems breakdown structure model and e-Government Relational Technical Security Controls model can alleviate this typical problem on information assurance projects. The relationships developed in the taxonomy will highlight the relationship between the different technical security controls for an information assurance project. The PMBOK Guide states, "frequent discussions about risks make it more likely that people will identify risks and opportunities" (PMI, 2008, p.311).

Information in an organization has a life cycle that resembles the normal distribution curve per Ng R. (2009). We will expect the performance measures of information assurance project to have a correlation to the information life cycle. At different stages of the information life cycle, its associated intrinsic value changes, thus it is fitting that we use the total cost of protection to optimize the appropriate security mechanism to maximize the effects of the security protecting information and information systems.

To be effective in our implementation of security programs or implementing security on a project we need to be aware that 'effective security implementation demands a holistic and systematic design and implementation' as Ng R. (2009) puts it. We need to move away from a reactive research approach for information assurance to a proactive approach. We need to establish security metrics that can be used to measure the performance of information security systems (Jaquith 2007). The project can be

modularized into measurable tasks and we can use Tan's (2002) methodology for assessing the risk to the project.

2.9 Federal Information Security Management Act 2002

In 2002 the Senate and House of Representatives of the United States of American Congress and the President of the United States, enacted the Federal Information Security Management Act of 2002 (FISMA) also commonly referred to as the E-Government Act (Pub. L. No. 107-347). This act emphasizes the importance of information security to the economic and national security interest of the United States. In summary, the act requires that all federal agencies and federal government contractors develop, implement, and document their information security program that manages the risk posed to information, information systems, operations and assets of the agency, other agencies, contractors and other sources of information.

The burden of implementing and ensuring the success of FISMA lie on agency program officials, chief information officers, the inspector general office (IG), the National Institute of Standards and Technology (NIST), the Office of Management of Budget (OMB) and federal government contractors. Their tasks include ensuring agencies conduct an annual review and audits of their information security program, develop controls and test standards for information systems, oversee and annually reporting on the compliance or non-compliance of federal agencies and contractors to the United States Congress.

The OMB uses this information to oversee the different programs and to prepare its annual report to Congress on the compliance or non-compliance of organizations to the e–Government Act. FISMA requires that the head of each federal agency implement policies and procedures that cost-effectively mitigate information security risks for their agencies to acceptable levels.

NIST is also a major player in the annual reporting activities of FISMA as they are responsible for developing guidelines, methodology, techniques etc for efficiently protecting federal information, information systems and assets. This collaborative

effort between NIST and federal agencies ensures that the agencies have a proper understanding of how the NIST guidelines can help them meet the FISMA requirements. NIST publishes these guidelines under the NIST Special Publication 800 series documents. NIST performs its statutory responsibilities through the Computer Security Division of the Information Technology Laboratory. The NIST mandate excludes all national security systems.

The security assessment performed on the information systems is to ensure that confidentiality, integrity and availability of these systems meet the technical, management and operational controls provided by the NIST guidelines. Confidentiality of information ensures that only entities (individuals or systems) with defined privileges and a need-to-know have access to certain information. Integrity is required to ensure the quality or state of the information is whole, completed and uncorrupted. Availability ensures that stakeholders and entities that should have access do have access to the system when they need information or services.

Annually, agencies and organizations expend extensive effort and resources to meet the FISMA 2002 requirements. Yet the controls use a one-size-fits-all approach to information assurance and in some cases, all the controls are not applicable to all information systems all of the time. An inordinate amount of time, effort and resources is expended in performing security assessment of information systems that are not applicable to the configuration of the information systems. A typical example will be using the controls for Anti-Virus software to assess the security posture of Cisco routers that do not run anti-virus applications. There is a need to develop a customizable methodology that can effectively assess the risk posture of an enterprise or project based on its information systems.

Prior to the release of the NIST SP 800-53 Rev 3 in August 2009, seventeen security controls were used to assess the security posture of information systems. In the recent release of the NIST SP 800-53 Rev 3, a Program Management (PM) control family was added to the seventeen controls bringing the number of security controls that

needs to be assessed for security compliance for all Federal Agencies and Federal Government contractors to eighteen. The addition of a Program Management control should sensitize us to the fact that NIST has recognized the need to program management methodologies for effective risk management.

NIST has made an attempt to identify controls that are systems-specific, common and hybrid. Yet no attempt has been made to classify the controls based on their application to specific types of information systems that may be used on projects or for enterprise networks. This research shall establish a basis for categorizing the controls based on their applicability to the different information systems that may be used on a project or that may exist in an enterprise.

2.10 Current e-Government Security Assessment Model

NIST has done extensive work in the development of security controls for assessing information systems. The sources of the security controls include defense, audit, financial, healthcare, intelligence communities, national organizations and international standards organizations. Some of the functions of the current model include:

- Identification of the need for organizations to identify common controls, hybrid controls and system specific controls
- Establishment of the Minimum Security Requirements for Federal Information and Information systems documented in the FIPS 200
- Establishment of Standards for Security Categorization of Federal Information and Information Systems documented in the FIPS 199
- Establishment of a security assessment framework for determining the effectiveness of security controls documented in the NIST SP 800-37

The current NIST security assessment controls comprise of the management, operational and technical control families depicted in Figure 2.1 and are decomposed

into the management, operational and technical security controls shown in Figure 2.2, Figure 2.3 and Figure 2.4 respectively.

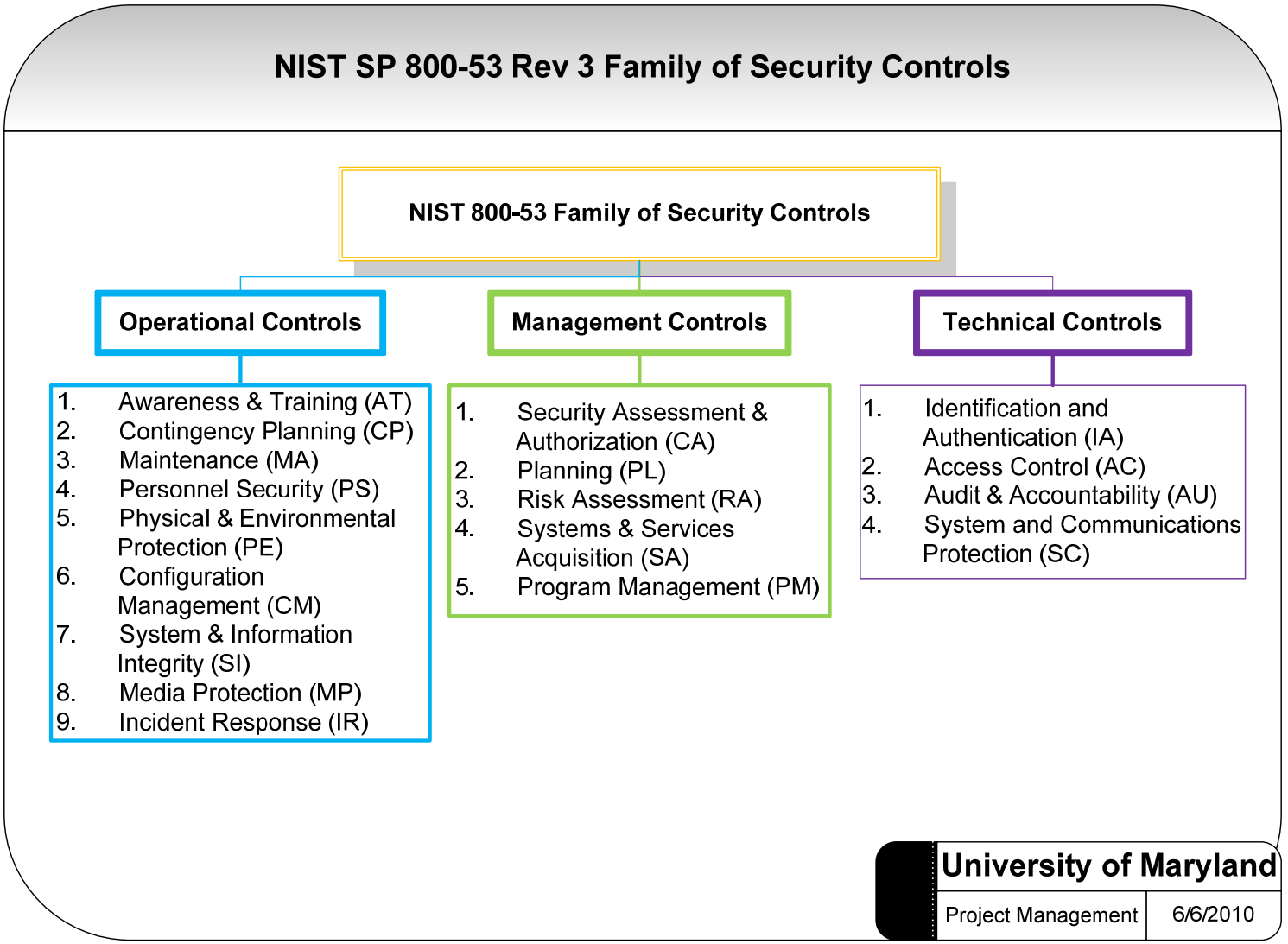

Figure 2.1 NIST SP 800-53 Rev 3 Security Controls

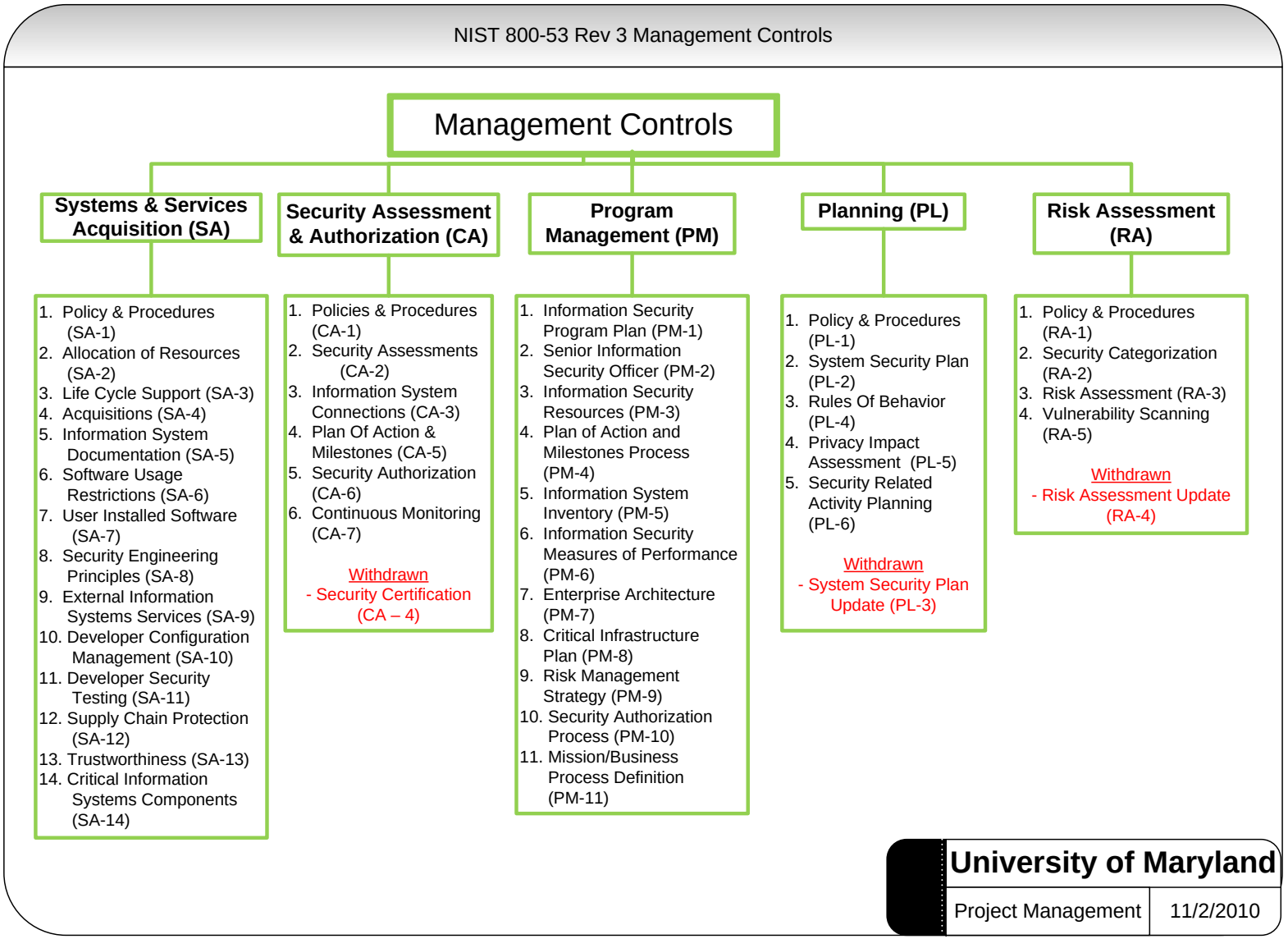

Figure 2.2 NIST 800-53 Rev 3 Management Controls

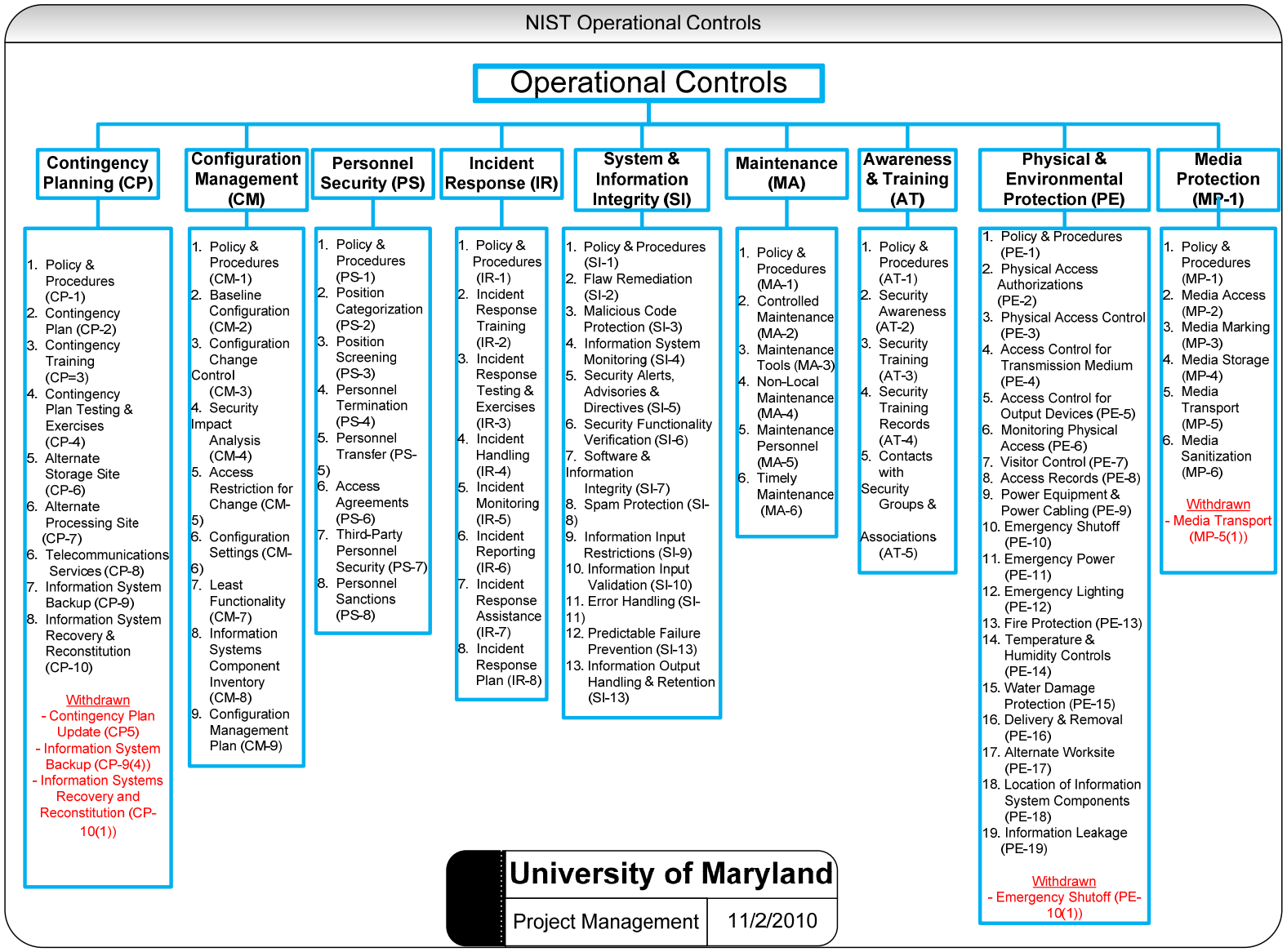

Figure 2.3 NIST 800-53 Rev 3 Operational Controls

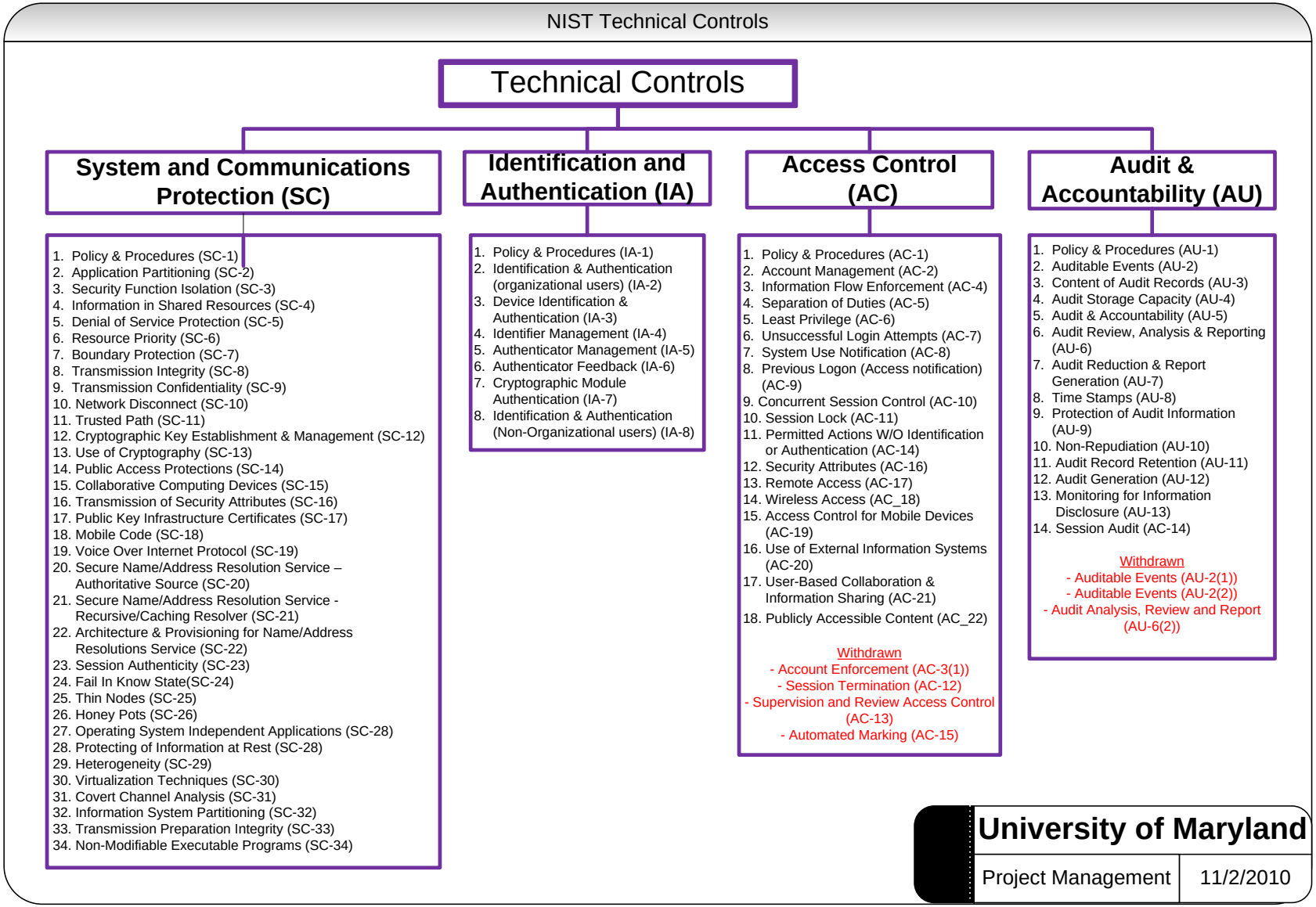

Figure 2.4 NIST 800-53 Rev 3 Technical Controls

The NIST hierarchical approach to security assessment of the controls is shown in Figure 2.2, Figure 2.3 and Figure 2.4 for the Management, Operational and Technical Controls respectively. NIST uses a hierarchical tree structure approach to identify and assess the different security controls. The assessment utilized is not relational and resulted in duplication of security controls. This duplication is documented in the NIST Special Publication 800-53 Rev 3 that was release on August 2009, by fifteen security controls that are withdrawn and merged into other controls. The fifteen withdrawn controls include the following:

1. Access Enforcement (AC-3 (1))
2. Session Termination (AC-12)
3. Supervision and Review Access Control (AC-13)
4. Automated Marking (AC-15)
5. Auditable Events (AU-2 (1))
6. Auditable Events (AU-2 (2))
7. Audit Analysis, Review and Report (AU-6 (2))
8. Security Certification (CA-4)
9. Contingency Plan Update (CP-5)
10. Information System Backup (CP-9 (4))
11. Information Systems Recovery and Reconstitution (CP-10 (1))
12. Media Transport (MP-5 (1))
13. Emergency Shutoff (PE-10 (1))
14. System Security Plan Update (PL-3)
15. Risk Assessment Update (RA-4)

A typical process flow for performing security assessment, based on the current NIST Risk Management Framework is shown in Figure 2.5. The second row contains the titles of actors that are typically involved in the security assessment process that include:

- Information System Owner

- Information System Security Officer (ISSO)
- Chief Information Officer (CIO)
- Senior Information Security Officer (SISO)
- Information Security Architect
- Common Control Provider
- Authorizing Official
- Security Control Assessor (also called Information Security Contractor)

The workflow process that supports the risk management framework is manual and consequently fraught with errors, delays and lacks transparency. There is no mapping of the information systems to their corresponding security controls. Most Federal Government enterprise systems are extensive and incorporate a 'spaghetti-network' of technologies that are obsolete and difficult to integrate. This is combined with the fact that the general workforce is aging and the baby-boomers are coming close to retirement. There is difficulty in maintaining appropriate staffing levels coupled with discontinuity and ineffective transfer of knowledge. This results in complex systems being administered and managed by novel personnel that do not have the expertise to make judicious decisions for security management. The development of an intelligent decision support system will make a difference in helping novice employees with the decision-making process required to support such large enterprise environments that typically have over five thousand users.

To be effective in performing security assessments, information security contractors need readily available current information on how Federal Government enterprises map to the appropriate security controls. Without this information, it is difficult to develop a test regime that reflects the configuration of an organization's enterprise. Consequently, we encounter several cases wherein performing security assessment has become a process of paper-trail documentation with very little or no impact on improving the security posture of the organization's enterprise.

The size and number of applications used by Federal Agencies necessitates the need to have multiple organizations performing concurrent security assessments on an infrastructure. This often results in cases where the number of personnel involved in the security assessment may disrupt Internet access by a denial of service attack due to limited or no communications between the security assessments teams. Some organizations have started designing and testing dashboards for tracking and controlling the multiple risk assessments but this was done without validating the security controls. This can result in the case of garbage-in and garbage-out if the design is not streamline to the information systems in use within the organization and its organizational policy.

A detailed discussion of the tasks for the risk management framework is documented in the NIST SP 800-37, as its discussion is beyond the scope of this research. It is important that we highlight the swim lane that contains the actor Security Controls Assessors. This lane identifies the tasks that information security contractors are typically subcontracted to perform on behalf of organizations.

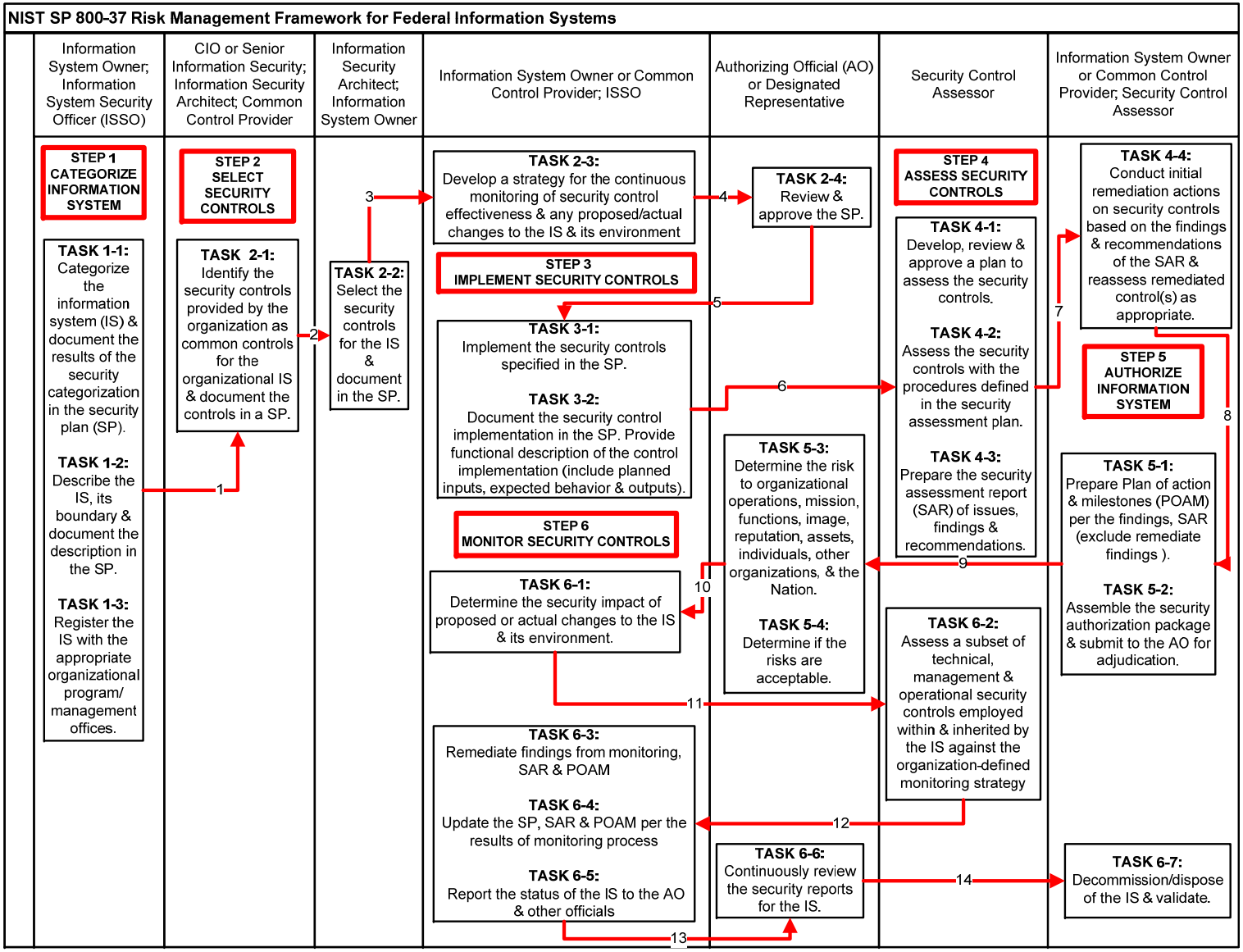

Figure 2.5 NIST SP 800-53 Rev 3 Risk Management Framework Process

2.11 Application of the e-Government Relational Model

In an attempt to address the application of the e-Government Relational Technical Controls taxonomy, the researcher provides the list below as a justification for development and application of this taxonomy.

1. It will improve communication between the customer, security experts, project managers and pertinent stakeholders on information assurance contracts because it will provide a common lingo to all participants
2. It will provide metrics and a methodology for meeting the different information assurance statutory requirements for information systems risk management
3. It can form the basis for establishing standards for performing security assessment of different information systems used on projects and found in the enterprise environment
4. It will assist personnel responsible for managing contracts to efficiently define the scope of work by using this e-Government Technical Controls taxonomy in the establishment of information assurance contracts and for managing and controlling information assurance projects
5. It can be use as a detailed level glossary of terms as it provides not only the definition of terms but also the relationships between information assurance entities.
6. The analytical model can be used in the process of developing a project management plan for managing project organizational risks on Federal Government projects. The cost model can be used to calculating the costs for performing security assessments for different types of information systems
7. The risk mitigation and management strategies identified can be used for the different information system and then reused in developing industry best practices for mitigating and managing risks to the different information systems utilized on projects
8. The e-Government relational technical controls taxonomy can also be use for teaching of information assurance at institutions, universities and on-the-job training.
9. It can be used to develop a responsibility matrix for information security assessment of Federal Government Agencies.

10. It can form the basis for the development of a decision-support system for security assessments
11. It can be used to develop a dashboard that provides a project status for the different information system security assessments in an organization.

Chapter 3 e-Government Relational Taxonomy Model

Chapter 1discussed the objectives, questions, scope and methodology of the research while Chapter 2 provided an overview of the literature reviewed for this research. This chapter will review the development of the e-Government Relational Technical Control taxonomy for performing of security assessment for Federal Government Information Assurance Contractors.

3.0 Definition of Terms for the e-Government Taxonomy

The website www.pcmag.com defines Information Assurance as "The technical and managerial measures designed to ensure the confidentiality, possession or control, integrity, authenticity, availability and utility of information and information systems. This term, which has spread from government use into common parlance, is sometimes synonymous with information security. The Department of Defense Information Assurance Workforce Improvement Program (DoD 8570.01-M) defines Information Assurance as "measures that protect and defend information and ISs by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of IS by incorporating protection, detection, and reaction capabilities."

Information Security is defined by US Code in [44 U.S.C., Sec. 3502] as the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity and availability. Information security and information assurance are closely related and sometimes the terms are used interchangeably in industry but there are subtle distinctions between the two. The next section shall identify the subtle distinctions between the terms though this is not the focus of this research. This research focuses on the development and validation of the information system breakdown structure, its mapping to applicable e-Government relational technical security controls and risk managements strategies.

The relationship of information assurance to information security is such that Information Assurance is a subset of information security. Figure 3.1 shows the relationship between Information Assurance and Information Security. Information Assurance involves ensuring the confidentiality, availability and integrity of data and information, which is a subset of Information Security. Information security encompasses ensuring the confidentiality, availability and integrity of data and information plus authentication, authorization, auditing and identification for information systems.

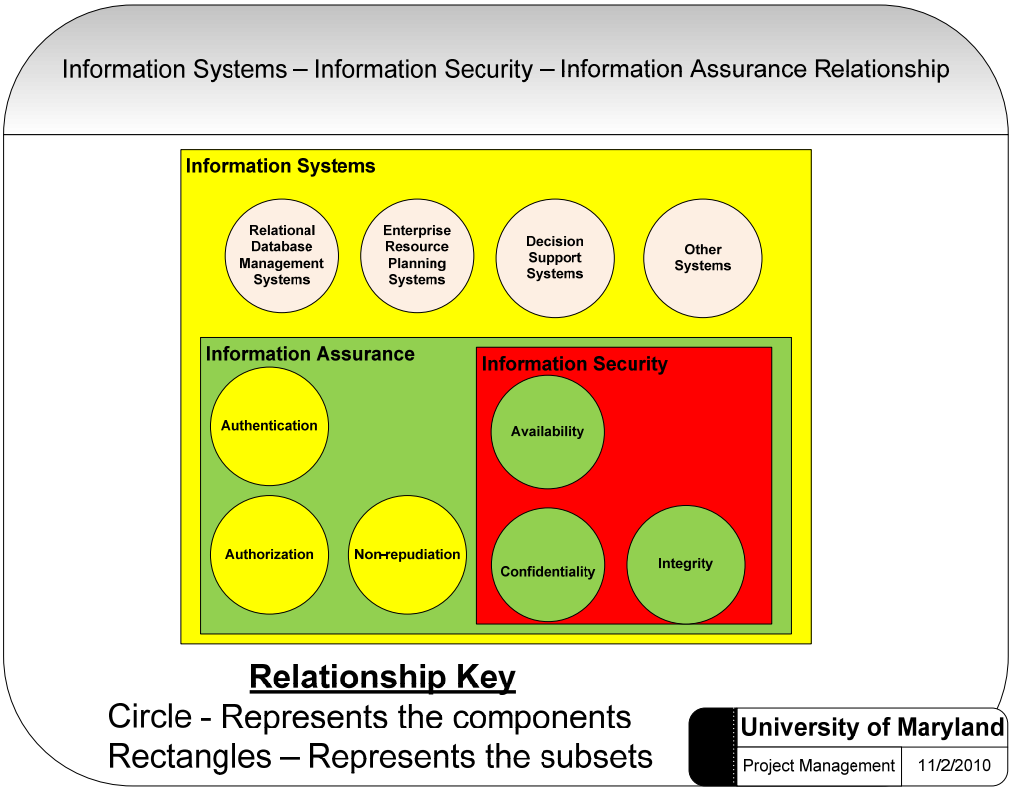

Figure 3.1 Information Assurance and Information Security Relationship

3.1 Information Systems Breakdown Structure (ISBS) Assumptions

The assumptions for the information systems breakdown structure include:

1. The environment comprised of computers, directory servers, application servers, database servers, web servers, print & file servers, faxes, scanners and printers.

2. The network infrastructure is comprised of switches, routers, firewall, telephony, storage area networks, tape backups, virtual private network devices and intrusion detection/prevention devices.
3. The servers and computers on the network are running Anti-virus software and other applications.
4. A single organization is responsible for policy development, implementation and management for all systems that make up the information systems breakdown structure.
5. The similarity in the physical characteristics of File & Print Servers, Application Servers, Database Servers, Web Servers and Directory servers make is possible for them to be grouped together as servers.
6. Personal computers are sufficiently different enough from servers in their functional use, though they have similar physical characteristics and security requirements. The requirements for personal computers and servers on the network makes then sufficiently different to be regarded as separate entities in the ISBS.
7. Mainframe computers are sufficiently different from servers in their architecture and administration for them to be included as a separate entity in the ISBS.
8. The network infrastructure source of vulnerability is similar enough for them to be grouped within the same entity in the ISBS.
9. Scanners, printers and faxes are similar in the protocols they use (i.e. IP and IP telephony) and thus their vulnerability source are similar enough for them to be grouped in the ISBS.
10. Scanners do not require user authentication prior to their use.
11. Printers are appearing on the market that have operating systems, so we assume that the printer group has an operating system as it is easier to include the attribute now than it is to add one at a future time.

3.2 e-Government Relational Technical Controls Taxonomy

Table 3.1 highlights the two models that make up the e-Government Relational Technical Security Control Taxonomy for performing information systems security assessments.

Table 3.1 e-Government Relational Technical Controls Taxonomy Model

#	Name	Purpose	Justification
1	Information System Breakdown Structure Model	A hierarchical chart that identifies the information systems that may be use for a project or that may exist in an organizations enterprise. It depicts systems at the category level, their associated sub-category, components and sub-components. The questionnaire was used to validate the structure and value of using this model.	This ensures that all the sources of information systems risk to a project or organization are be properly identified with a goal of mitigating and managing them. It also provides a method to assign responsibility and track security assessments for the systems. The information systems breakdown structure then maps to the Systems/Devices entity of the e-Government Relational Technical Controls Model
2	E-R Diagram for the NIST Technical Security Controls Model	An entity relationship diagram that identified the entities and relationships between the entities for the technical security controls. This provides a way to track the controls to the information systems identified in the ISBS and the users.	This method uses a relational approach to information systems security assessments. It assesses the relationships between the entities of the Technical control family and provides an opportunity to assess the attributes of the entities and easily relate them to attributes of other entities. The diagram also depicts the cardinality between the entities. The relationships were developed based on discussion with industry personnel on the possible cardinality between the entities. In cases where the researcher had to chose between a zero to one relationship as opposed to one to multiple relationship, the researcher choose the zero to one relationship because it was the trivial option of the two.

The questionnaire included items that validated the relationships and attributes of the identification and authentication entity of this model. Questionnaire items for the Access Control, Audit and Systems and Communications Entities were developed and are provided in Appendix B. These items were excluded from the scope of the research to ensure the number of items in the questionnaire did not exceed 100 or else it would have been impossible to find respondents for the questionnaire.

3.3 Information Systems Breakdown Structure

In project management, we observe the use of several breakdown structures. These include the work breakdown structure, the risk breakdown structure and the organizational breakdown structure. These breakdown structures have one very important function: decomposing project tasks, risks or roles into smaller manageable portions that can be tracked, controlled and measured to improve communications and efficiency, as well as assign responsibility & authority for the different sub-entities.

Mantel et al 2005 maintains, *"Inadequate up-front planning, especially failing to identify all important tasks, is a primary contributor to the failure of a project to achieve its cost and time objectives."*[i] The work breakdown structure is the cornerstone of project management and it consistently adds value to the process of managing projects through its efficient use. Can a similar model for the information system breakdown structure help us identify information system risk for a project or an organization?

Kerzner (2006) observes, "The first major step in the planning process after project requirements definition is the development of the work breakdown structure (WBS). A WBS is a product-oriented family tree subdivision of hardware, services and data required to produce the end product."

The WBS pictorial is developed to include all the required tasks to produce a product, deliver a service or deliver a project. The finished product, delivered service or deliverables of the project are listed at the top of the tree and decomposed into smaller manageable and measurable tasks. The WBS tasks are then transformed into a sequenced diagram like the Gantt chart or a bar chart that can be used to track project metrics.

The '100% rule' for a WBS indicates that the summation of the entire child work component should be equal to the effort required for delivery of the parent

component. In addition, the WBS should include all the work defined by the project scope and identify all the project deliverables. The WBS should capture all the work to be performed to successfully complete the project.
The tasks to be delivered by the WBS should be mutually exclusive. The WBS should not contain duplicate tasks or the risks for assigning responsibility to multiple people increases thereby resulting in communication challenges and the likelihood of having duplicate charges that will result in errors in the cost estimates. When the WBS elements names are ambiguous, then a WBS dictionary must be developed to address the definition of the WBS elements.

I am proposing the Information System Breakdown Structure depicted in Figure 3.2, with a goal to identify all the information systems required to support a project and ensure the confidentiality, integrity and accessibility of data while maintaining the non-repudiation of tasks during the course of the project. With the information system breakdown structure (ISBS), we can use the concept of "divide and conquer" wherein we decompose the architecture, design, process, procedures, and implementation of information systems so that we can better understand and manage the risks associated with the different components.

In the current practice of project management, we assess the risk posed to the project due to cost, time, quality and ensuring customer satisfaction. In many cases, we forget that an equally important area of project management is composed of the information systems that make the managing of complex projects feasible. We also tend to neglect that fact that without sufficient security imposed on the information system component of the project, the risks of a project failing increases.

Project managers should start identifying, assessing and managing the risks posed to the project due to their choice of information systems used on a project. In that light the research presents Figure 3.2 as the first iteration of the information system breakdown structure. This is a living model that should be customized for a project or organization and updated as newer technologies are added to the information system

landscape of project. It can then be used to assign responsibility for performing security assessment for the different security teams and highlight the relationships between the different systems.

The goal in the development of an information system breakdown structure is to decompose the category of information systems into its sub-categories, components and sub-components that are typically used on most projects, most of the time to access, share, support and manage project information. The sub-categories are decomposed into the main components that make up the information system breakdown structure. Further decomposition of the components into sub-components highlights the sub-components that are assembled to make the main component.

Threats to information systems used on a project can come from any sub-category, component or sub-component levels so it is important that we identify these entities and their associated source of risks (threats) for the different information systems utilized on projects. Park (2009) states "The best defense against Web-based attacks it to know where the most vulnerable areas of a system are." Part of the process of identifying the most vulnerable areas of the system involves understanding the components that makes up the system and their inherent vulnerabilities.

Some of the sub-components like protocols, and applications have a tendency to appear in other components. As a result, these sub-components have been assigned a generic outline level containing an X to indicate that it may take component level numbers. The information system category is decomposed into the following sub-categories:

1.1 Computers
1.2 Network infrastructure
1.3 Personal digital assistants
1.4 Imaging devices
1.5 Other devices

The following sections shall further discuss each of the sub-categories and their corresponding components and sub-components as detail in Figure 3.2.

Computers

The sub-category of computers for the information systems breakdown structure is used to refer to any system that has a central processing unit and a human-computer interface that includes a mouse, keyboard and a display screen. The term computer is used very loosely and it is not to be confused with the term 'personal computer'. The computers section is typically made up of the following hierarchy:

1.1.1 Personal Computer
1.1.X.1 Hardware
1.1.X.2 Operating System
1.1.X.3 Applications
1.1.X.4 Protocols
1.1.X.5 Firmware
1.1.2 File & Print Server
1.1.3 Application Server
1.1.4 Database Server
1.1.5 Web Server
1.1.6 Directory Server
1.1.7 Mainframes
1.1.8 Virtual Machines

Within the Personal Computer component are the hardware, operating system, applications, protocols and firmware sub-components that go towards making the personal computer. All of the sub-components of the personal computer exist in the component for File & Print Server, Application Server, Database Server, Directory server, Mainframes and Virtual Machines. To avoid the need for duplication of these sub-components they are listed with the component of Personal Computers as 1.1.X.1 to 1.1.X.5 also apply to the parent components within the computers sub-category.

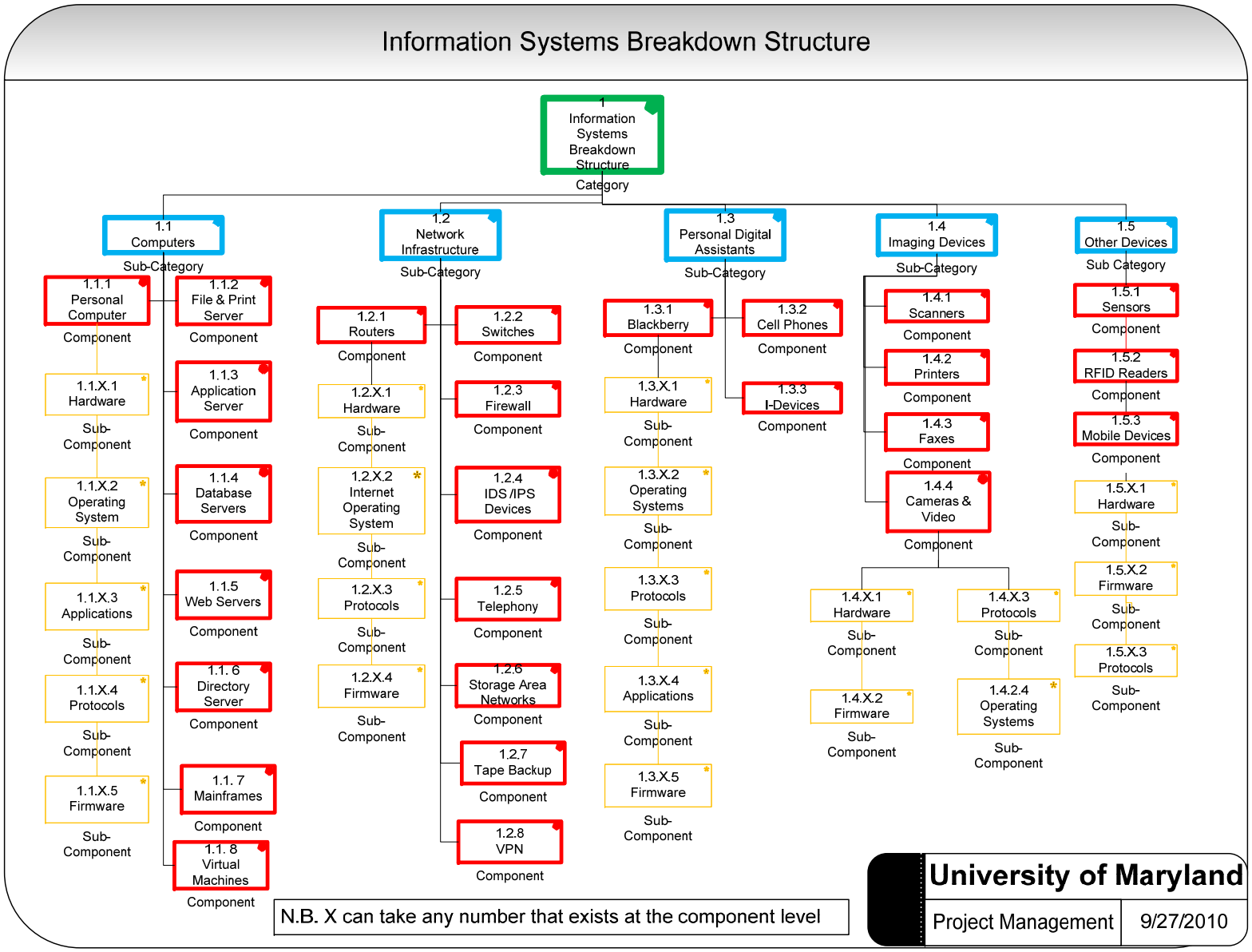

Figure 3.2 Information System Breakdown Structure

The sub-component of Hardware can be further decomposed into the different modules and sub-modules that make up the Personal Computer. There are risks associated with the module and sub-module levels. These modules typically include the CPU, hard drive, motherboard, etc but the purpose of this research, we have chosen to stop at the hardware sub-components level so that we can concentrate on the goal of mitigating risk to the project. Risks posed by the hardware sub-component are usually addressed in the contingency and disaster recovery plan for the various systems and incorporated into the business continuity plan for the organization.

Network Infrastructure

The sub-category of network infrastructure for the information system's breakdown structure is used to refer to local area network (LAN), metropolitan area network (MAN) or wide area network (WAN) that the computers are connected to so that they can communicate with each other and with other systems outside of the enterprise. Some of the components typically found in the network infrastructure for most projects include:

1.2.1 Router

1.2.X.1 Hardware

1.2.X.2 Internet Operating System (IOS)

1.2.X.3 Protocols

1.2.X.4 Firmware

1.2.1 Switch

1.2.3 Firewall

1.2.4 Intrusion Detection System/Intrusion Protection System

1.2.5 Telephony

1.2.6 Storage Area Networks (SANs)

1.2.7 Tape backup

1.2.8 Virtual Private Networks (VPN)

Routers are typically made up of hardware, an Internet Operating System (IOS), protocols for routing and routed protocols and the firmware. These sub-components

(hardware, IOS, protocols & firmware) exist in the components of switches, firewall, storage area networks, IP telephones, intrusion detection system (IDS) and intrusion protection systems (IPS). Hubs are the only components that do not have an IOS but it has all of the remaining sub-components. Switches have replaced hubs in most organizational information system infrastructure due to their design, which creates single broadcast and collusion domains, often resulting in heavy network congestion. Hubs are only included for completion but they are typically not found on projects or organizational networks.

Personal Digital Assistants (PDA)

The line dividing computers from personal digital assistants (PDAs) is becoming blurred with the development of mobile computing operating systems that fully integrate with the network infrastructure. However, they are still a different line of components because of their smaller size and limited functionality compared to what can be accomplished on a computer. PDAs may come in the form of Blackberry, cell phones, i-Devices and other devices. Others include items that have a similar functionality but may be marketed under different brand names. The components for the sub-category of PDAs include:

1.3.1 Blackberry
1.3.X.1 Hardware
1.3.X.2 Operating System
1.3.X.3 Protocols
1.3.X.4 Applications
1.3.X.5 Firmware
1.3.2 Cell phones
1.3.3 i-Devices

PDAs come in different forms, shapes and with varying functionality but their goal of keeping the user organized with reminders has not changed. Most of them now include applications that allow a user to make online purchases for airline tickets, schedule meetings, check emails, review project documents, perform presentations

etc. Examples of i-Devices include iPods, iPad and iPod Touch. Examples of other devices include the Kindle, which is an Internet enabled device with a similar functionality to i-Devices, in that they are both capable of making online purchases.

Imaging Devices

The sub-category of imaging devices in the information systems breakdown structure is used to refer to the category of systems that produce or can be used to input or transfer images to the sub-category of computers. It is primarily made up of peripheral devices that are typically neglected in most security assessments yet they are systems that can easily be hacked because no security protocols are being developed for these devices, which are not required to authenticate to the network. Typical examples include:

1.4.1 Scanners

1.4.2 Printers

1.4.3 Faxes

1.4.4 Cameras and videos

1.4.X.1 Hardware

1.4.X.2 Firmware

1.4.X.3 Protocols

For most information systems networks, these devices are configured as network devices and in some cases, they are configured as wireless devices and may act as major sources of threat to the network. In addition, when it comes to management of network devices, the firmware running on these are rarely upgraded, either due to lack of knowledge of the threats these systems may pose or because of limited maintenance and management policies for these systems that extend beyond replacing paper/ink or break-fix repairs.

Cameras and videos were added based on feedback received during the pilot testing of the questionnaire. They are often configured in promiscuous mode to accept all

incoming calls and for ease of use. This has the effect of them being used a readily available bug for meetings.

3.4 Entity Descriptions

This section presents the descriptions of the entities and their attributes identified in Figure 3.3. It also shows how the information system breakdown structure may be related to the e-Government Relational Technical Controls Model via the System/Device entity.

User/Processes Entity

People that access the information system either locally or remotely are referred to as users for this research. They may include contractors, vendors and the public. The interaction of users with the system is restricted to the input, output and transformation of data and information. They have no rights to manage the system. This definition of users excludes system maintainers that may require a different set of access control to the information system.

Processes for this research are batch or scheduled jobs that need an identifier to validate their authenticity so that they can run on the information system. The users may come from the organizational chart that can be used to assign groups and roles for the information system. Project Management currently utilizes the organizational breakdown structure to assign responsibility for tasks on the work breakdown structure. The organizational breakdown structure can also be used to assign the controls that apply for the different users within and outside the organization.

System/Devices Entity

System and devices include computer, network devices, PDA, imaging devices and other devices from the information system breakdown structure that may have a media access card, wireless access card or connection that can access the information system locally or remotely

Identification & Authentication (IA) Entity

The identification and authentication entity is responsible for capturing the attributes for identification and authentication between the information system and users, processes, devices or other system. The primary attribute of the identification and authentication entity is to establish and manage unique identifiers of users, processes, devices or other systems that may access the information system.

Other attributes of this entity include multi-factor authentication management, obscuring of feedback, encrypting of the passwords in transit and identification and authentication of non-organizational users. Figure 3.3 contains a detailed list of the attributes of this entity. For a discussion of the different controls and enhancements for this attribute see the NIST SP 800-53 Rev 3.

Access Control (AC) Entity

The access control entity is responsible for capturing the attributes that regulate access to components of the ISBS, after they have been identified and authenticated. The primary role of the access control entity is for managing (granting/denying) access to entities that may want to access/utilize the information system and its components.

Additional attributes for this entity include the management and enforcement of accounts, managing of information flow between secure and non-secure areas of the information system, ensuring separation of duties for personnel, defining how unsuccessful login attempts should be handled, providing system use notification, presenting previous logon information to the user prior to granting access to the information system. Managing of session lock, identifying actions that do not require authentication to the information system, specifying how remote and wireless access is monitored and managed.

Access control also covers the requirements for the use of mobile devices on the network, specifications for the use of external information system and public access to information. Figure 3.3 contains a detailed list of the attributes of this entity.

Audit & Accountability (AU) Entity

The audit and accountability entity is responsible for monitoring the access granted or denied by the access control entity for entities that have completed the identification and authentication process with the information system and its components.

Attributes for the audit and accountability entity include auditing events, establishing the content of audit records, and ensuring there is sufficient space on the system to store audit records and their corresponding storage duration. It also includes ensuring that a process is in place for reviewing, analyzing and reporting on audits, establishing time stamps, protecting all audit information, ensuring that the audit records can meet the requirements for non-repudiations, monitoring of information disclosure and monitoring of audit sessions. Figure 3.3 contains a detailed list of the attributes of this entity.

System & Communications Protection (SC) Entity

This entity is responsible for tracking of auditing records and is based on a set of criteria or rules, performing actions to maintain the security posture of the information system. This entity is capable of artificial intelligence since it is based on the audit records, which are analyzed to identify patterns and develop rules for information system. It can also support decision support systems for decision making for the other entities due to its ability to synthesize extensive audit records.

Attributes of this entity include ensuring that secure and non-secure applications are appropriately partitioned, implementing security function isolations, preventing denial of service, identifying resource priority, and establishing trusted paths for data communications. Additional attributes include managing of cryptography, public key infrastructure, managing mobile code and ensuring the integrity, confidentiality and

availability of data during communications and in-situ. Figure 3.3 contains a detailed list of the attributes of this entity. The System & Communication Protection entity also has the greatest potential to utilize artificial intelligence and manage the interactions between the other entities.

3.5 E-R Diagram for the E-Government Technical Controls

Table 3.2 presents the relationships between the different entities of the e-Government Relational Technical Controls Model. It also discusses the cardinality between the entities.

Table 3.2 From Entity – To Entity Relationships

From Entity	To Entity	Relationship
Users/Processes	Identification &Authentication	A user/process must have (and be restricted to) a unique identifier that is use to authenticate to the information system.
Identification &Authentication (IA)	Users/Processes	The IA Entity can identify and authenticate only systems/devices (i.e. no users/processes) or many users/processes.
System/Devices	Identification & Authentication	A system/device must have (and be restricted to) a unique identifier that is use to authenticate to the information system.
Identification & Authentication	System/Devices	The IA Entity can identify and authenticate only users/processes (i.e. no system/devices) or many systems/devices.
Identification & Authentication	Access Control	An authenticated identifier may be granted access to one or many information systems
Access Control	Identification & Authentication	Access Control manages the access of one or many authenticated identifiers.
Audit & Accountability	Access Control	Audit & Accountability tracks the access of one or many authenticated identifiers.
Access Control	Audit & Accountability	The access control entity logs to the audit & accountability entity the access utilization of one or multiple authenticated identifiers
System & Communications Protection	Audit & Accountability	Tracks the one or many audit & accountability logs and raises alerts, or makes information systems configuration changes based on preconfigured rules to manage the state of the

From Entity	To Entity	Relationship
		information system.
Audit & Accountability	System & Communications Protection	Monitors and logs one or many system and communication protection changes for the information system.

3.6 Identification & Authentication Risk Management Strategies

The NIST SP 8-53 Rev 3 controls for the Identification and Authentication control family was used to identify best practices for the identification and authentication risk management strategies. Questionnaire items were developed to validate the identification and authentication best practices for risk management. Interview items were also developed for the Access Control, Audit and Systems and Communications Protection Entities but they were excluded from the interview process to prevent the questionnaire items from exceeding a hundred items. The questionnaire for this research is included in Appendix A and the excluded questions are documented in Appendix B.

The questionnaire items were preceded with the associated NIST control ID that generated the risk strategy. The questions included issues related to identifier generators and management, single-sign on, one-time passwords, periods of inactivity, characteristics for user passwords and cryptography. Information security contractors with extensive expertise in identification and authentication were asked to select whether they strongly disagree, disagree, agree or strongly agree with the position presented for identification and authentication risk management. The identification and authentication control family items that were used to identify risk mitigation and management strategies are documented in Section 3 of the questionnaire documented in Appendix A.

A list of effective identification and authentication risk management strategies that were significantly based on the analysis of the questionnaire are presented in Chapter 5 of this dissertation.

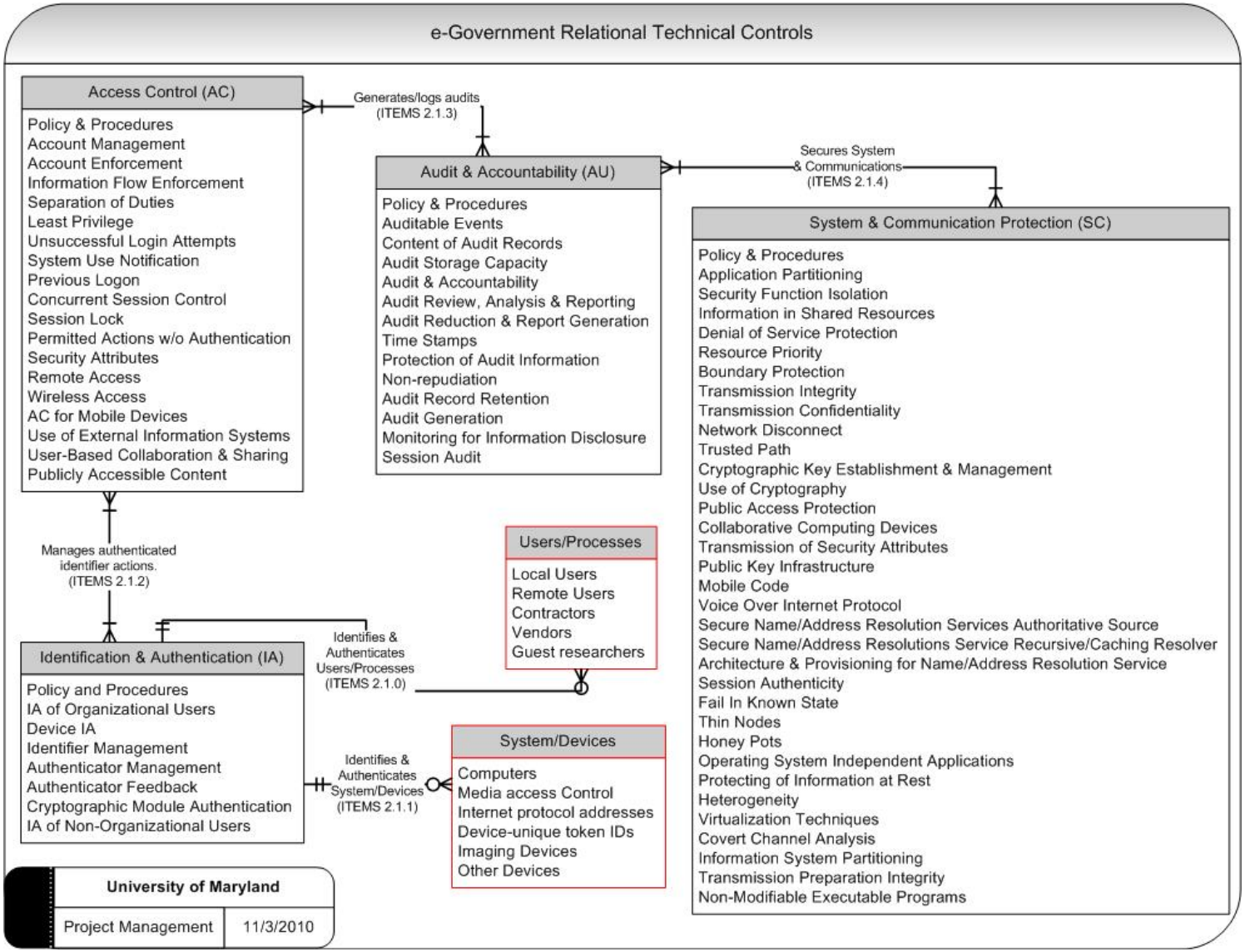

Figure 3.3 e-Government Relational Technical Controls Model

3.7 Identification & Authentication Security Assessment Costs

This section discusses the development of the model for determining the cost of performing security assessment for the identification and authentication control family and its attributes. The researcher discussed with industry experts to identify the typical tasks and durations used to perform security assessment tasks for the identification and authentication control family. This guided the selection of the tasks and the duration ranges for the hours specified in the questionnaire. The questionnaire also included items to determine the hourly rates paid by Federal Government Agencies for security assessment of their information systems.

Ng R. (2009) states that "Before we can effectively deal with the design and deployment of security solutions, we need to understand the value of the underlying information assets that need to be protected." Gordon (2002) developed an economic model to determine the optimal amount that organization should invest in information security. This work is not directly applicable to the research as the research is interested in process costs for performing security assessments as opposed to information technology assets cost.

Ng R. (2009) maintains that "the cost of security protection should never exceed the sum total of the value of the information." This means that after implementation of the security controls, the Information Assurance systems should audit the Deployment Ratio ($D_{R)}$ to ensure that the implementation follows the policy guidelines and specifications. The deployment ratio ensures that the company resources are judiciously utilized so without overspending on protection and exceeding the value of the information. It is all well that we may want to limit our spending on protecting our information system but we should also be aware of the risks, litigations and compensation costs that the organization may be exposed to if we are found to be negligent.

The questionnaire items that were developed to establish an agreed-upon duration for performing security assessment for the identification and authentication security

controls are documented in Appendix A. The tasks for which the durations were collected were based on the NIST guidelines for the risk management framework documented in the NIST SP 800-37. The questionnaire items include questions related to the duration for reviewing and assessing documentation, developing and administering security tests, performing interviews and developing reports for the identification and authentication control family. The respondents were asked to respond to the questions based on the last security assessments they performed, which included the identification and authentication control family. Analysis of the responses obtained from the questionnaire collection is documented in Section 5 of this document.

3.8 Hierarchical e-Government Model Vs Relational e-Government Model

Table C62 (in Appendix C) compares the current hierarchical e-Government model against the relational e-Government Model. It highlights the advantages and disadvantages of using a hierarchical e-Government model against a relational e-Government model.

Chapter 4 Information Assurance Data Collection

This chapter discusses the development and data collection process of the questionnaire that included:

- Validating the information system breakdown structure model
- Validating the e-Government Technical Security Controls Taxonomy
- Validating the Identification and Authentication Control risk management strategies
- Identifying the duration for the tasks and associated costs for performing security assessments using the current methodology

This section discusses the architecture of the questionnaire, the targeted respondents, questionnaire distribution, responses received, problems encountered, validity and reliability of the data collection questionnaire. The researcher pre-screen the questionnaire respondents to ensure they are have the skills and expertise to understand the questions, diagrams and statements used in the questionnaire. Responses that were incomplete and did not meet the minimum requirements for inclusion in the questionnaire were excluded from the research analysis. A copy of the questionnaire used for this research is included in Appendix A of this document. Questions in Appendix B were not included in the questionnaire to reduce the length of the questionnaire. These questions are included in this document for future research.

4.0 Design of the Data Collection Questionnaire

Following the development and refinement of the information system breakdown structure and the e-Government relational model, a project-level data collection questionnaire was develop and pilot tested before being used in the data collection process. Several methods for administration of the data collection effort are available but a self-administered questionnaire was deemed most efficient for the availability and schedule of the respondents, low cost, large-geographic coverage, and ease of

implementation. The data collection questionnaire is shown in Appendix A of this document.

4.1 Structure of the Data Collection Questionnaire

The data collection questionnaire commenced with an introductory statement on why the respondent was selected for this voluntary data collection effort and how the data collected will be used. It also provided the contact information for the project supervisor. Following the introduction page, the data collection questionnaire was separated into the following four sections:

- Section 1 consisted of eighteen questions (Items 1 – 17) and collected personal information of the respondents. The data collected in this section included: the date, location, name, title and contact information of the respondent, as well as their experience with interpreting entity-relationship diagrams. The remainder of this section collected years of experience data from the respondents: as network administrators, network security, FISMA, performing security assessment and their past information assurance projects. The questionnaire also collected information on industry-recognized security certificates and level of education, and had an option for the respondent to provide additional information on their expertise in applying security to information assurance related projects. This information forms the basis for comparing the responses to the other sections of the questionnaire. It was also used to assess the significance of the different experience of the respondents.
- Section 2 collected information to establish the value of using the ISBS model shown in Figure 4.1, to identify and classify the organizational information system resources that may be utilized on a project. The section consisted of eight questions (Items 18 – 26) based on a 4-point (force-choice) Likert scale. The section asked respondents to determine whether they strongly disagree, disagree, agree or strongly agree with statements based on the ISBS. An example of the 4-point forced choice approach that was used is shown in Table 4.1

Table 4.1 Four-Point Forced Choice Likert Scale

		Strongly disagree	Disagree	Agree	Strongly agree
42.	The access control entity must create an audit event record.	○	○	◉	○

The 4-point forced choice approach was used to divert respondents from taking the path of least resistance by choosing a middle category. It also allowed the responses to be dichotomized into two groups of agree or disagree. Respondents were provided an option to provide feedback on their responses to ensure that they have an opportunity to express views that were not capture using the Likert 4-point (force-choice) scale. This ability to clarify their responses allowed the respondents to focus to the next set of items while providing valuable information to the research on the choices of the respondents.

- Section 2 of the questionnaire was used to validate the relationships for the e-Government Relational Technical controls model. The section consisted of an entity relationship diagram of the e-Government Relational Technical Controls and the items in the data collection were developed to validate the relationships between the users/processes, system/devices, identification and authentication (IA), access control (AC), audit & accountability (AU) and the system & communication protection (SC) entities. The section consisted of twenty-five 4-point forced choice questions and feedback (items 27 to 51). The questions were developed so that can be answered independent of the respondents' knowledge of how to interpret the entity-relationship diagram shown in Figure 4.2. The relationships validated in this section of the questionnaire included:
    - Users/Process and IA Entity Relationships
    - System/Devices and IA Entity Relationships
    - IA and AC Entity Relationships
    - AC and AU Entity Relationships
    - AU and SC Entity Relationships

The section asked respondents to determine whether they strongly disagree, disagree, agree or strongly agree with the statements that establish the relationships between two related entities for the e-Government Relational Technical Controls. A forced-choice approach was used to prevent respondents from taking the path of least resistance by choosing a middle category. Respondents were provided an option to provide feedback on their responses to each set of relationship statements they disagreed with.

- Section 3 was used to validate the existing risk management strategies are used as attributes of the Identification and Authentication Entity of the e-Government Relational Technical Controls. The thirty-seven questions in this section cover item 52 to item 88. Respondents were provided an option to provide feedback for statements they strongly disagree or disagreed with for the identification and authentication risk mitigation and management strategies.
- Section 4 contained questions that will help develop a cost model for establishing the cost of performing security assessment for the identification and authentication control family. The six questions (item 89 to item 94) asked questions about the duration to:
    - Examine and assess documents related to the identification authentication control family
    - Interview organizational stakeholders on the requirements for identification and authentication control family
    - Test the control requirements for the identification and authentication control family
    - Develop report for the identification and authentication control family
    - Identify the last organization that the respondent performed a security assessment for that involved the identification and authentication control family
    - Identify the fee their organization charged for the last security assessment that involved the identification and authentication control family.

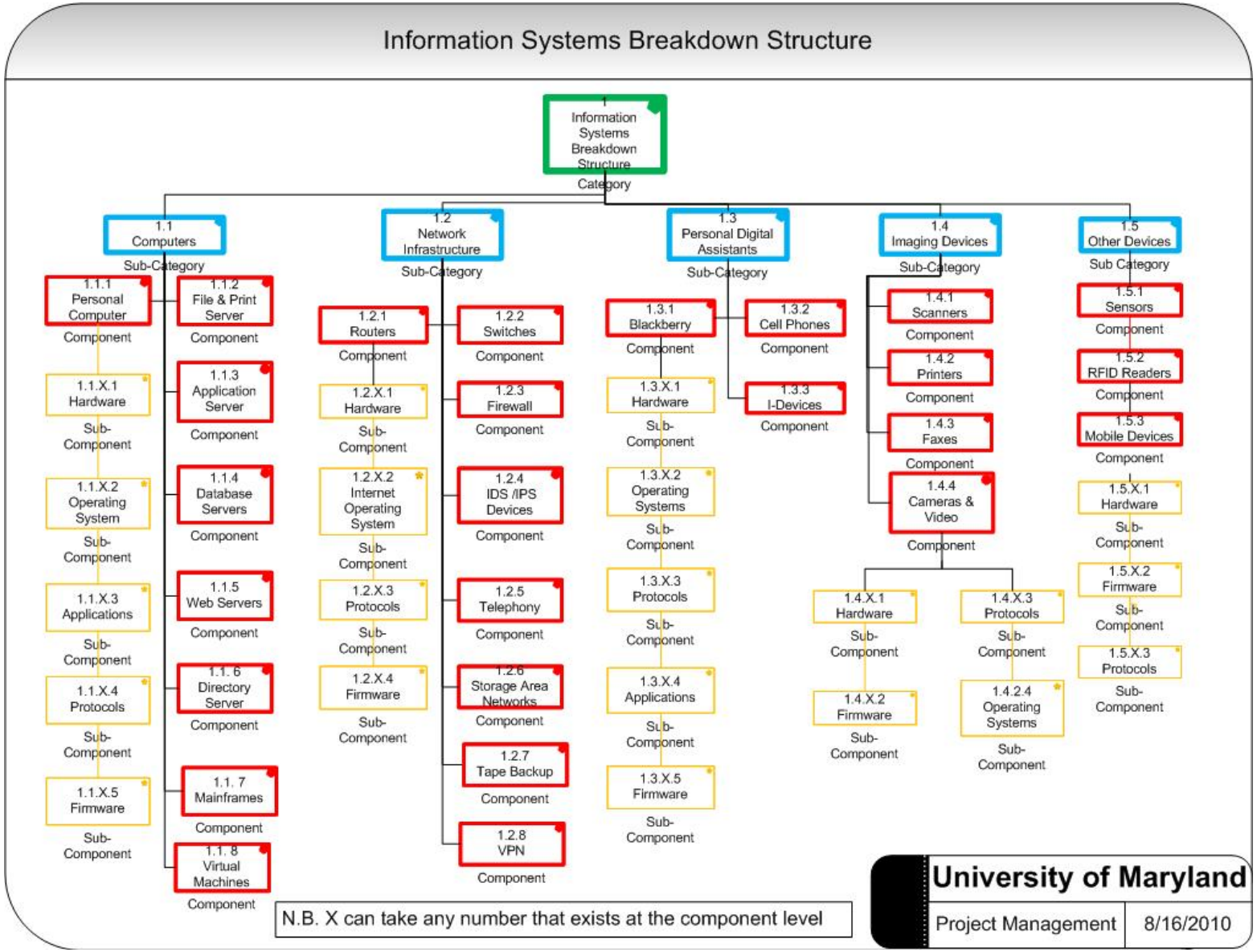

Figure 4.1 Information System Breakdown Structure

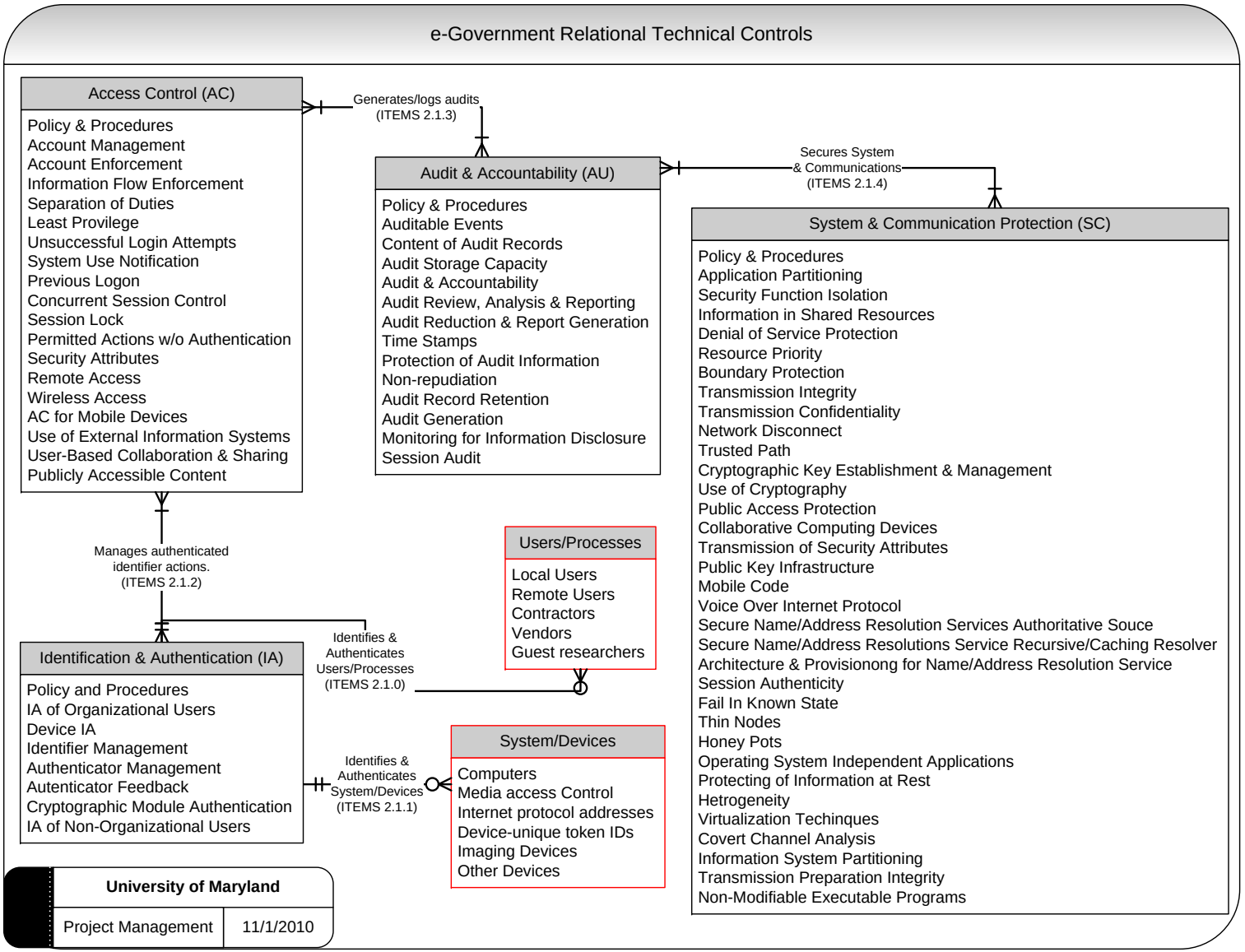

Figure 4.2. e-Government Relational Technical Controls

4.2 Initial Review of the Data Collection Questionnaire

Industry practitioners and academicians initially reviewed the data collection questionnaire. Detailed discussions about the questionnaire were made over virtual meeting sites like Skype and via email. The initial review helped to ensured the following:

1. The structure, wording, format and measurement scale of the questionnaire were clear, understandable and analyzable
2. The data required for the research could be obtained
3. The questions to validate the relationships between the entities did not require knowledge of entity-relationship diagrams
4. The technical content of the questions did not extend beyond the knowledge and expertise of the respondents
5. The questions were comprehensive and complete for the goals and objectives of the research
6. The format of the questions were clear and the answer choices did not lead to recording of wrong answers by the respondents
7. It was possible to provide a pictorial of the entity-relationship diagram for the e-Government Relational Technical Controls and the Information System Breakdown Structure
8. The likelihood of a web session timing out during the answering of the questionnaire online was minimized or responses being lost because they had not been recorded in the online database
9. Minimize the likelihood of receiving incomplete responses to the data collection questionnaires
10. Potential errors in recording were identified and resolved to minimize the effect of data errors

4.3 Email-based data collection questionnaire

Based on the comments and suggestions obtained from the initial review, it was decided to administer the data collection questionnaire via email. This limited the need for users to have a constant connection to the internet and the possibility that

their sessions will timeout after thirty minutes of inactivity. A measure that is controlled by the application service provider and that the researcher has no control over. In addition, it ensured that the contact information for the respondents was readily available and that the respondents do not have to complete the questionnaire in one sitting.

Over eighty percent of the questionnaires were self-administered; the respondents choose the best time to complete the questionnaire without having to factor in the availability of the researcher. With the widespread use of email and Internet technologies, distribution of the data collection questionnaire to the respondents was easy and inexpensive. Some of the advantages of using email and the Internet to distribute the questionnaire include low cost, quick turnaround time, prompt correspondence between the respondents and the researcher, unlimited geographic boundaries and user convenience.

4.4 Architecture of the Data Collection Questionnaire

The data collection questionnaire was developed using Microsoft Office InfoPath 2007 and its design controls that included check boxes, option buttons, text box, banners, pictures, tables, mail to and hyperlinks. The check boxes and option buttons were grouped and linked under the same categories for the different questions. This prevented the likelihood of a respondent selecting multiple answers for a single answer question while allowing them to select multiple answers for a multiple answer question. The forms that were developed in Microsoft Office InfoPath 2007 was then copied over to Microsoft Office Word 2007 and saved as a Word 2007 version (with .docx extension) and a Word 97 - 2003 version (with .doc extension).

The tables ensured that the responses were maintained in line with the responses and this limited the confusion over which responses went with which comments. The use of check boxes also limited the likelihood of the questions having random answer formats. Formatting tools and colors were used to highlight the different sections of

the questionnaires and breakup the monotony of using just black on white for the entire questionnaire. Figure 4.3 is a screen shot of the first page of the questionnaire.

As illustrated in Figure 4.3, the first page of the questionnaire explained the data collection objective, benefits, targeted respondents, and the contact information for the project supervisor. We also expressed appreciation to respondents for participating in the survey.

The rest of the data collection questionnaire flowed logically through the four sections of the questionnaire. Section 1 collected information on the respondents that would be used as a basis for analysis of the responses. Section 2 asked questions to validate the Information System Breakdown Structure. Section 3 asked questions to validate the relationships for the e-Government Relational Technical Controls model. Section 4 asked questions to determine the value of the current risk mitigation and management strategies for the Identification and Authentication Control family. There was ninety-five items in the questionnaire.

Questions were developed for the other three technical control families namely access control, auditing, and system and communications protection. These questions are included in Appendix B. Including the three control families in the questionnaire would have brought the total number of questionnaire items to over three hundred and it would have been impossible to find knowledgeable and willing respondents for the research. This happens to be one of the limitations of the research.

Except for two respondents that returned an incomplete questionnaire and a pencil-improperly marked questionnaire, all the respondents were included in the research because their work experience and expertise in information assurance had been pre-screened for their expertise in information assurance prior to them being invited to participate in the research.

e-Government Relational Technical Controls Data Collection

Dear Sir/Madam,

Based on your recognized expertise in information systems security you are kindly requested to participate in the **University of Maryland** research requiring data collection related to e-Government Relational Technical Controls. In our data collection effort, we ask information security industry experts such as yourself questions about the integration of the Identification and Authentication Control for the NIST SP 800-53 Rev 3 within information system(s) and assess the value of a relational model and an information system breakdown structure for performing security assessments. This data collection will require completion of this questionnaire.

Of course, your participation in this research effort is voluntary and the time taken from your busy schedule will be much appreciated. There are no foreseeable risks associated with this project. However, if you feel uncomfortable answering any questions, you can withdraw from the data collection exercise at any point. It is very important for us to learn your opinions on this subject.

Your responses will be strictly confidential and data from this research will be reported only in an aggregate form. If you have questions at any time about our data collection or the procedures, you may contact the project supervisor at the University of Maryland, College Park, Dr. M. Skibniewski at 301-405-9364 or by email (preferred) at mirek@umd.edu.

Yours sincerely,

Momodu Fofana, PhD C, MIS, B. Eng, PMP, CISSP, CCNA
Research Associate

Email: mfofana@umd.edu
Phone: (240) 533-6757

Figure 4.3 First Page of the Data Collection Questionnaire

The respondents held a minimum of a Masters Degree or PhD with extensive industry or research experience for security assessments. Respondents with a Bachelors degree needed to have over four years of experience performing security assessments to be included in the research. Some of the respondents held the industry-recognized security certificate of CISSP. Pre-screening the respondents ensured that they had performed security assessment and have a common understanding of the information assurance terminology and processes.

4.5 Pilot Testing of the Data Collection Questionnaire

The data collection questionnaire was pilot-tested with a sample of five respondents and the following modifications were made to the questionnaire to make it more user-friendly and to incorporate the multiple answers observed for some questions. Table C-61 (in Appendix C) depicts the changes that were made to the questionnaire. The 'Ques #' column identifies the item number that the change was made to, the 'Previous' column depicts how the question was formatted in the pilot and the 'Change To' depicts the changes that were made to the final questionnaire. These changes were reviewed and approved by the project manager. All subsequent questionnaires were based on the final questionnaire. Additionally, there were no drastic changes made to the content of the pilot questionnaire, responses in the pilot were modified to the updated questionnaire format and included in the analysis for the research.

4.6 Research Respondents

The target respondents were information assurance Federal Government Contractors and Employees. The respondents selected for inclusion in the research had the following characteristics:

- A Masters Degree or higher and some experience utilizing the NIST Security Controls or;

- A Bachelors Degree and over three years of experience performing security assessments using the NIST Security Controls

Pre-screening of the respondents ensured that they were familiar with Network Administration and security assessments using the NIST Security Control, prior to their inclusion in the data collection effort. Respondents were asked to answer project related questions based on the most recent information assurance project in which they participated.

Respondents were identified through the:

- Information Assurance experts that gave talks at conferences and seminars
- Inter Sec site at https://isc2intersec.leveragesoftware.com/login.aspx
- Information Assurance experts that the researcher was familiar with their work

The primary method for contacting respondents and inviting them to participate in the data collection effort was via the Inter Sec bulletin board, telephone or email. After a respondent agreed to participate in the data collection effort, they were sent a copy of the questionnaire in either Microsoft Office Word 2007 (extension .docx) and/or Microsoft Office Word 97-2003 formats (extension .doc). They were instructed that they only needed to complete one of the forms and the forms were to be returned back to the researcher by 9/3/2010. The diversity of the respondents from the different government departments and agencies, the random composition of information assurance projects and the requirement that they answer the questions based on the last project they worked on prevented respondents from being bias with their responses.

4.7 Questionnaire Distribution

Twenty-two of the respondents selected to participate in the data collection effort have performed security assessments on projects with the following Federal Government Agencies and organizations:

- Department of Defense

- Department of Homeland Security
- Department of Education
- United States Patent and Trademark Office
- Federal Aviation Administration
- Drug Enforcement Agency
- Department of Health and Human Services
- Department of Treasury
- Center for Medicaid and Medicare Services
- State of Florida
- Environmental Protection Agency
- Department of Labor
- National Oceanic and Atmospheric Administration
- General Service Administration
- NASA
- Executive Office of the President
- US Capitol Police
- Department of Interior (US Geological Survey)
- US Department of Agriculture
- Bank Of America

Respondents were emailed with a brief description and objectives of the research to enquire if they were available to participate in the research. Respondents who replied expressing an interest to participate in the research were emailed the two formats of the questionnaires with instructions for completing the questionnaire. The National Institute of Standards and Technology (NIST) Computer Division was invited to participate in the research via multiple emails but we did not receive responses from them. Other organizations invited to participate in the research include The Project Management Institute (PMI) and the International Information Systems Security Certification Consortium, Inc. $(ISC)^2$ The questionnaire was also uploaded at the following Inter Sec website of https://isc2intersec.leveragesoftware.com/login.aspx

4.8 Data Collection Questionnaire Responses

The pilot testing and data collection was conducted between August 7 2010 and September 3 2010. Twenty-four responses were received but two of the responses were rejected. The first response was rejected because the respondent had insufficient experience with the NIST Security Control Families to be included in the survey and the second response was rejected because the respondent had pencil marked the questionnaire with multiple answers that was confusing and some pages were missing from the final survey. In addition, responses received after 5:00 pm EST of September 3rd, 2010 were excluded from the research. The title that the respondents reported for the questionnaire included the following:

- CIO & Director/CEO (2)
- Computer Systems Analyst
- Systems Project Analyst
- Facilities Administrator IV
- Sr. Programmer Analyst
- Security Engineer/Auditor (3)
- Business Intelligence Consultant
- Sr. Systems Programmer/Engineer
- Sr. Enterprise Architect
- Contract Security Office for Department of Home Land Security
- VP Of Technology Operations
- WAN Engineer
- IT Specialist
- Information Systems Security Manager (ISSM)
- Information Systems Architect/Information Assurance SETA
- Information Assurance Analyst
- Sr. Network Security Engineer

Figure 4.4 depicts the distribution of the respondents based on the questionnaire classification of project manager, information security contractor, network engineer

(this included the network administrator classification), and other categories. Sixteen respondents classified themselves as information security contractors, three of them classified themselves as network engineers, while the remaining three were classified as other.

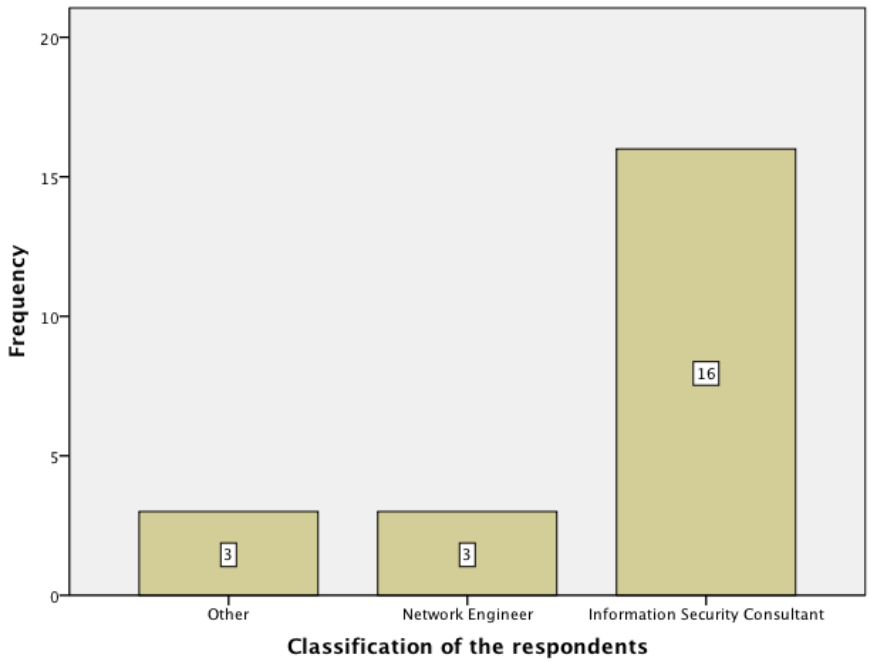

Figure 4.4 Classification of the respondents

The respondents that classified themselves are other were a programmer, a systems project analyst and a physical security officer. All of whom play very important roles in information assurance. The difference in responses between those that classify themselves as "Other" and those that classify themselves as "Information Security Contractors" was not significant for exclusion of the other responses from the research. The diversity of the expertise of the respondents resulted in very interesting feedback. Figure 4.5 shows a crosstab distribution of the different categories and their expertise with entity-relationship diagrams.

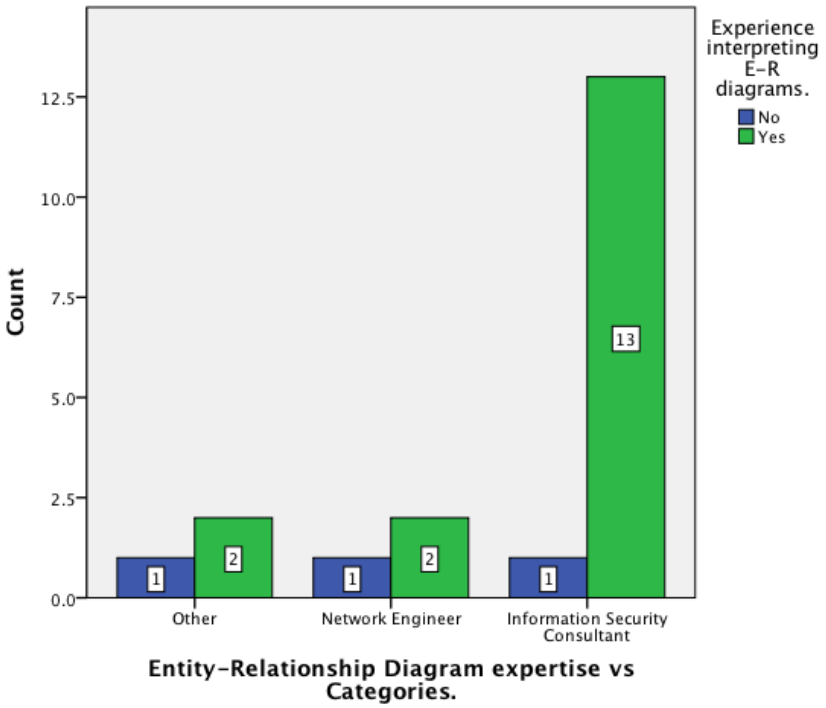

Figure 4.5 Entity-Relationship Diagram Expertise vs Categories

Each of the three groups had a respondent without expertise interpreting E-R diagrams. In addition, a Chi-square test of the significant of those with and without E-R diagram experience gave (chi-square (1) = 9.80, p =.002). This means that we have 99% confidence that the respondents with E-R diagram experience are significant.

Respondent experience information for network administration, network security, FISMA and security assessment was assessed next and the modal mark for all categories was found to be the four to eight years experience.

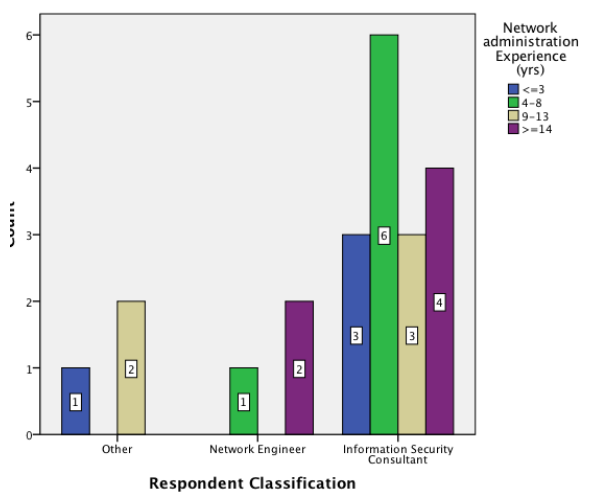

Figure 4.6 Network Administration Experience

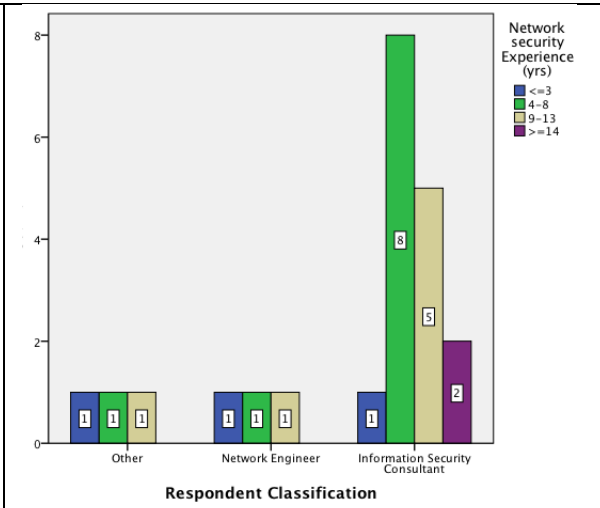

Figure 4.7 Network Security Experience

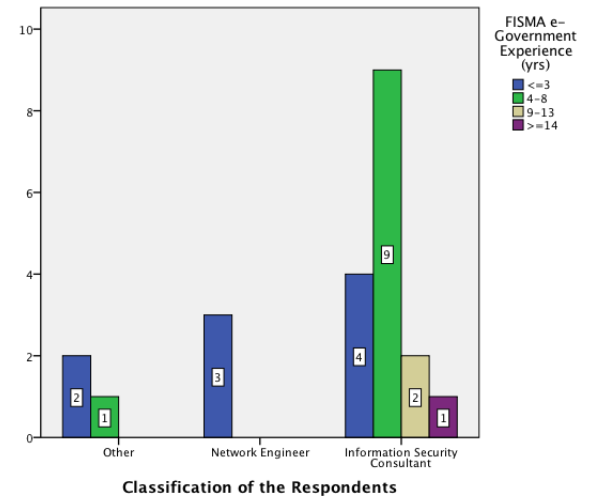

Figure 4.8 FISMA Experience

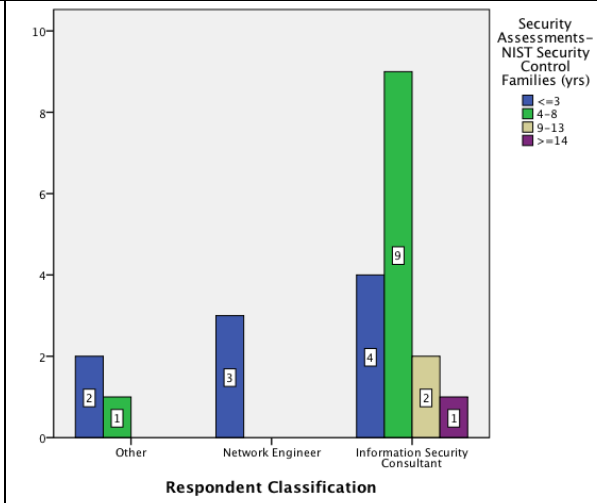

Figure 4.9 Security Assessments Experience

Figures 4.6 to 4.9 show the years of experience of the respondents for network administration, network security, FISMA/e-Government and network security assessment. We observe from the four graphs that the modal mark lies in the information security contractors' category with expertise of four to eight years. We also observe that the graphs for the information security category appear to be positively skewed distribution with the peak (highest frequency) on the left-hand side. In order to have exactly 50 percent of the distribution on each side, we can deduce that the median must be located to the right of the mode. In addition, the mean will be located to the right of the median because it is influenced by the extreme scores and will be displaced further to the right by the scores in the tail. This means we can expect to find the median of our responses to be from information security contractor with 9 years or more expertise in the four different areas.

The degrees, industry recognized certification and years of experience performing security assessment distribution for the respondents is shown in Table 4.2 The CISSP certification is the modal certificate for the respondents. The total of industry certifications was twenty-three averaging a certificate per respondent.

Table 4.2 Respondent Degree

Degree and Certificates	Count
Bachelors Degree	**5**
<=3	**2**
None	2
4-8	**3**
CISSP	1
CISSP, PMP	1
Other	1
Masters Degree	**14**
<=3	**5**
CISSP, PMP, ITIL V2	1
MCSE, Security +	1
None	2
Other	1
4-8	**7**
CISSP	1
CISSP, MCSE	1
CISSP, Security +, ITIL Foundations	1
MCSE, PMP, CCNA, CCNP	1
None	2
PMP	1
9-13	**2**
CISSP, PMP, NSA-IAM	1
MCSE	1
Post Graduate	**1**
<=3	**1**
MCSE	1
PhD	**1**
<=3	**1**
Other - Not specified	1
Grand Total	**21**

4.9 Problems Encountered During the Research

Some of the problems encountered during the research include:

- The Microsoft Word 2007 document took long to load/open because it had radio buttons, check boxes and text fields. This happened to be the problem most reported by the respondent. The questionnaire was saved in Microsoft Word 2003 format that was easier to load.
- An incomplete questionnaire was received from one of the respondents so their responses were rejected
- A poorly pencil marked questionnaire with missing pages was received from another respondent so their responses were rejected
- Another respondent had problems marking the responses using Microsoft Office Word 2007 because macros was disabled on their system, so they printed the questionnaire and properly marked the answers on the paper, scanned and emailed a pdf version of the questionnaire to the researcher
- Experience several failed attempts to create the questionnaire online with the following specific problems:
    - Free sites like Google docs did not allow pictures to be uploaded to their site and the recommended workaround did not work and would have required the respondent to have multiple windows open at the same time
    - The online sites had session timeout configured so several questions were created that did not post to the website and had to be recreated. This resulted in a loss of time and lots of frustration for the researcher, as well as in the questionnaire being created on the local computer of the researcher using Microsoft Office InfoPath 2007. In most cases, it appeared as if information technology was part of the problem instead of a catalyst to the research
    - The online fee for services sites were cost prohibitive to provide the same functionality provided using Microsoft Office InfoPath.
- Respondents were not too keen to provide the hourly rate their organizations charged for performing security assessments. The research used the hourly rates

provided by select respondents and validated the information against GSA Schedule rates for information security contractors.

4.10 Reliability and Validity of the Data Collection Questionnaire

The two key characteristics of a questionnaire are its reliability and validity. Psychometrics was performed on the questionnaire to assess its reliability and validity prior to its use for data collection.

4.11 Validity of the Data Collection Questionnaire

Validity is a measure of whether a test is measuring what it is intended to measure and it is affected by reliability. Reliability is a necessary but insufficient condition for validity. Fink (2009) maintains that 'A valid survey is a reliable one, but a reliable one is not always valid.' A survey is valid if the information it provides is an accurate representation of the respondent's knowledge, attitudes, values and behavior. Some characteristics of surveys include:

- predictive validity (ability to predict future performance)
- concurrent validity (shows a strong correlation to existing validated surveys for the same group or validating the scores against experts' judgments of respondents' attitudes)
- content validity (by proving that its items accurately represent the metrics they intend to measure)
- construct validity (by testing the survey on respondents with known characteristics based on expert recommendations, to validate the survey)

Blerkom (2009) states that a good test should evenly sample the domain and that such a test would display content-related evidence of validity. An even distribution of questions within the domains for the information systems breakdown structure, the entity-relationship diagrams and the risk mitigation and management strategies for the identification and authentication security control family.

"The four types of validity are construct validity, content validity, concurrent validity and predictive validity." (Christmann 2009) Construct validity is based on how closely a test measures a theoretical construction and the degree of accuracy between a test and the construct it is designed to measure. Christmann states, "A simple way of determining construct validity is to correlates tests' results with the results of reputable tests that have established construct validity." (Christmann 2009). Construct validity is the most valuable and difficult to assess and it is often determined after years of experience with a survey.

Content validity is a subjective measure of how the questions seem to a set of reviewers who have knowledge of the subject matter. Two common tests of content validity are face validity and sampling validity. Face validity is based on the investigator's and industry experts' subjective evaluations. Sampling validity ensures the population is adequately sampled by a questionnaire and it is commonly used when investigators attempt to construct and utilize a questionnaire for the first time.

Empirical validity decomposes into concurrent validity and predictive validity. It assesses the relationship between a questionnaire and its outcomes. Concurrent validity assesses the validity of a questionnaire against an existing 'proven' questionnaire for measuring the same subject. Predictive validity assesses the correlation coefficient between the results of a questionnaire and an external criterion and it is used to forecast future outcomes.

The pilot test included procedures to assess the questionnaires validity and reliability prior to its use. The questionnaire was assessed using content validity, as no golden standard questionnaire exists to perform a concurrent or construct validity tests. Predictive validity is not applicable for this type of research due to the dynamic characteristic of information assurance. What may be considered a secure mode today could be an unstable/unsecure mode six months later. The two tests of content validity performed include face validity and sampling validity, which shall be discussed in the subsequent sections.

Face validity for the data collection questionnaire was established by performing the following:

1. A comprehensive literature review and unstructured interview of industry practitioners was conducted to ensure the information system breakdown structure develop was comprehensive, the entity-relationship diagram for the NIST Technical security controls were comprehensive and included all the current attributes and the risk mitigation and management strategies assessed are proven and established in the information assurance industry. To establish the baseline cost model for the tasks and durations based on security assessment of the identification and authentication control family.
2. Feedback and comments collected through the expert discussions and unstructured interviews were used to refine the research model and a pilot test of the questionnaire was performed. The results of the pilot test resulted in minor modifications to the questionnaire format to improve consistency in responses, formatting and clarity of the questions.

Sampling validity for the data collection questionnaire was established by performing the following:

1. Ensuring that the respondents to the questionnaire worked in the information assurance or related industry and had experience with performing security assessment using the NIST special publications guidelines.
2. The questionnaire asked questions of the number of years of experience respondents had with network administration, network security, FISMA, security assessments and the corresponding number of projects completed. This was done to validate the sample of the population and the analysis was performed on their responses to ensure that their years of experience was significant and showed alpha less than 0.05.
3. Only completed, valid and timely responses were included in the analysis of the results.

4.12 Reliability of the Data Collection Questionnaire

Reliability is synonymous with consistency. It indicates the ability to repeatedly measure the same variable and get the same results. Fink (2009) states that, 'A reliable survey provides a consistent measure of important characteristics despite background fluctuations.' Variance in samples is explained by reliability. The observed variance (for our sample) is equal to the true variance plus the error variance. The error variance is a measurement of the error and causes an observed score to differ from a true score.

$$\text{Variance}_{\text{observe}} = \text{Variance}_{\text{true}} + \text{Variance}_{\text{error}}$$

$$\text{Reliability} = (\text{Variance}_{\text{True}}) / (\text{Variance}_{\text{Observed}})$$

Reliability can range from zero to one. When measuring human psychological characteristics, such as knowledge or ability, it is extremely difficult to develop tests with reliabilities above 0.90. (Blerkom 2009) It is quite difficult to measure the $\text{Variance}_{\text{True}}$ of any sample. Reliability can be measured by several methods depending on how frequently the questionnaire is administered. If the questionnaire is administered more than once, a test-retest method can be used to assess the correlation between the sets of scores. In addition, multiple questionnaires for the same criteria but worded differently, can be developed to measure the same criteria and an alternate-form method can be used to assess the correlation between the two forms of the questionnaire. The final method to assess the reliability of the questionnaire is the split-half method that splits the responses into two halves and assessing their correlation.

The split-half method results in measures given by the Spearman-Brown metric were used to measure the correlation between nominal variables for this research. Cronbach's alpha coefficient is a revision to the Spearman-Brown formula to estimate the reliability of a questionnaire using the split-half method. To assess the reliability of the questionnaire, Cronbach's alpha coefficient was used since the survey was only

given once to respondents and the scale of measurement was ordinal. The values obtained and depicted in Table 4.3 are high for sections two, three and four with the questions in section one in the acceptable range of 0.50 – 0.60 suggested by Kaplan and Saccuzzo (1993). The values indicate that the questions utilized have a very high reliability to be reproduced or can be included in the questionnaire. Cronbach's alpha was calculated using SPSS version 18.0.

Table 4.3 Cronbach's Alpha Coefficients for the Data Collection Questionnaire

Sections and Related Questions	Valid Cases	Number of Items	Cronbach's Alpha Coefficient
Section 1			
Questions related to the years of experience with network administration, network security, FISMA and security assessment for the respondents	22	4	0.519
Section 2			
Questions related to validating the information system breakdown structure.	22	8	0.911
Questions related to the Entity-Relationship Diagram for the NIST Technical Controls	22	20	0.914
Section 3			
Questions related to the Risk Mitigation and Management Strategies for the Identification and Authentication Control Family	22	37	0.913
Section 4			
Questions related to the duration for performing security assessments	20	4	0.740

Chapter 5 Data Analysis and Results

This chapter discusses the results obtained from the analyses of the data collected during the data collection effort. The chapter begins with descriptive statistics of the respondents, their expertise in network administration, network security, security assessments and FISMA. The descriptive analysis includes highlights the different organizations for which the respondents have performed security assessments in the past.

This chapter also reviews factor analysis, and correlations for the information systems breakdown structure, the e-Government Relational Technical Control and salient risk mitigation and management practices gleamed during the data collection exercise. The results obtained from factor analysis, which were performed in order to determine the components that improve an information system security posture, the associations and correlations are highlighted.

5.0 General Characteristics of Respondents

The general information on the respondents, collected during the data collection effort include their current job title, job classification, expertise with Entity-Relationship diagrams, education, number of information assurance projects completed and years of experience with network administration, network security, FISMA and security assessment.

Twenty-five responses were received for this data collection effort. One of them was rejected for having several incomplete sections for the questionnaire. Another response was rejected for improper markings (multiple answers to the same question that were pencil marked) and the third was rejected because it was received after the deadline for receipt of responses. The remaining twenty-two respondents were analyzed and selected for inclusion in the data analysis and results.

5.1 Job Classification and Education of the Respondents

Figure 5.1 illustrates the highest level of education achieved by the respondents. Of the twenty-two respondents, one had a PhD degree, sixteen had Master of Science degrees and five had Bachelor of Science degrees. We observe that over 75% of the respondents have at least Masters Degrees and the remaining respondents holding Bachelors Degrees.

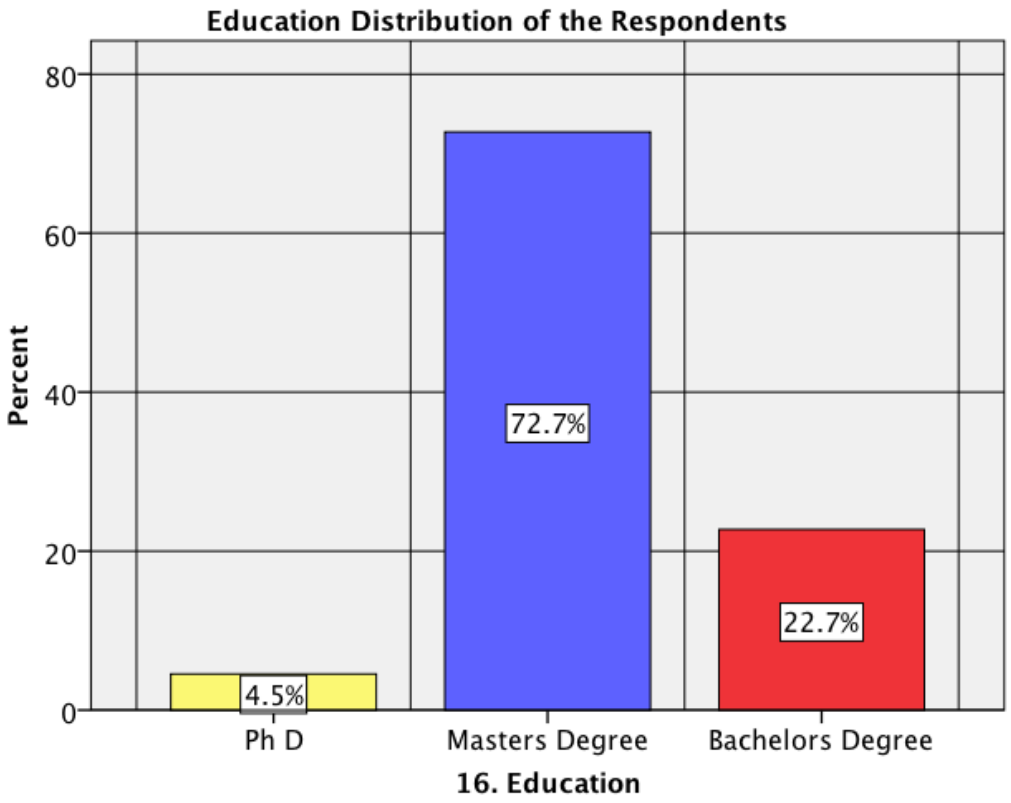

Figure 5.1 Highest Education Level of the Respondents

The respondents were asked in the data collection questionnaire to select all the classifications that apply to their job title, from a list of project manager, information security contractor, network engineer, network administrator and other. Figure 5.2 shows the rankings for the different job classifications selected by the respondents as:

- Eleven Information Security Contractors (50%)

- Three Others – This was comprised of respondents with job titles of Programmer, Systems Project Analyst and Contract Security Officer (14%)
- Two Network Engineers (9%)
- Two Project Managers/Information Security Contractors/ Network Engineers/Network Administrators (9%)
- A Project Manager (5%)
- A Network Administrator (5%)
- A Project Manager/Information Security Contractor (5%)

We observe that fifty percent of the respondents classified themselves as exclusive Information Security Contractors. We also note that approximately seventy percent of the respondents considered their jobs to include the job functions of an Information Security Contractors.

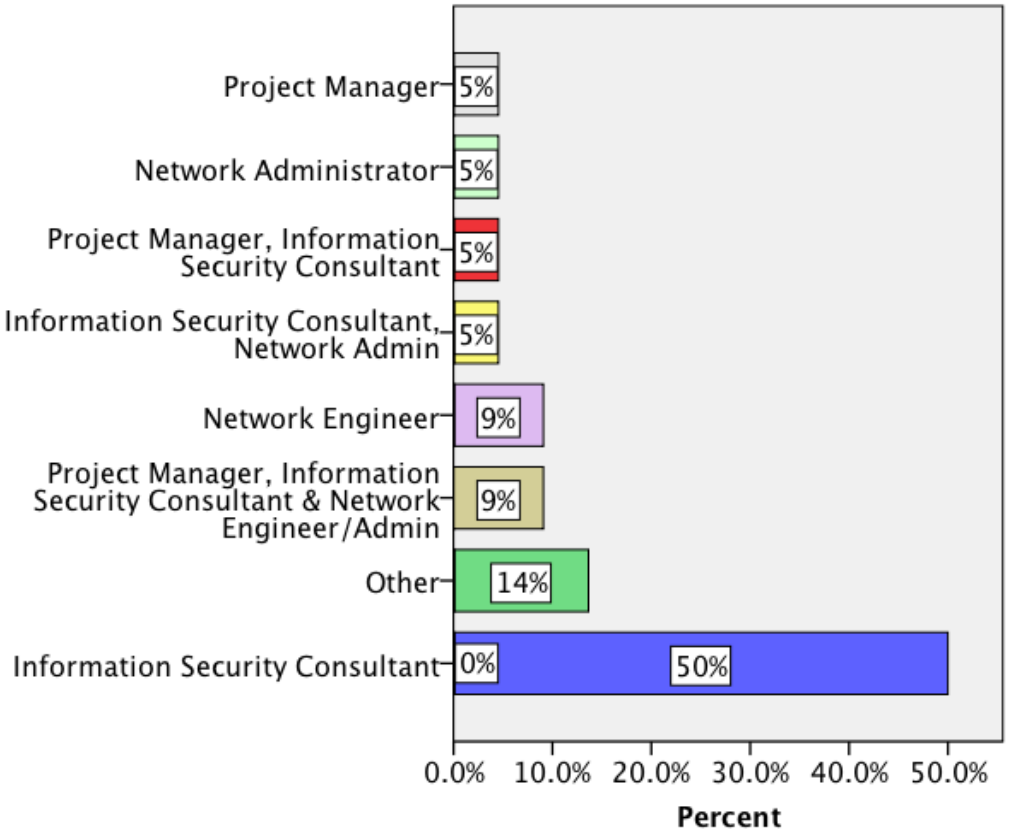

Figure 5.2 Job Classification of the Respondents

Further decomposition of Figure 5.2 to see the educational composition of the different job classifications is shown in Figure 5.3. We observe that all the Bachelors Degree respondents have the exclusive job classification of Information Security Contractor. The remaining respondents had a Masters Degree or a PhD.

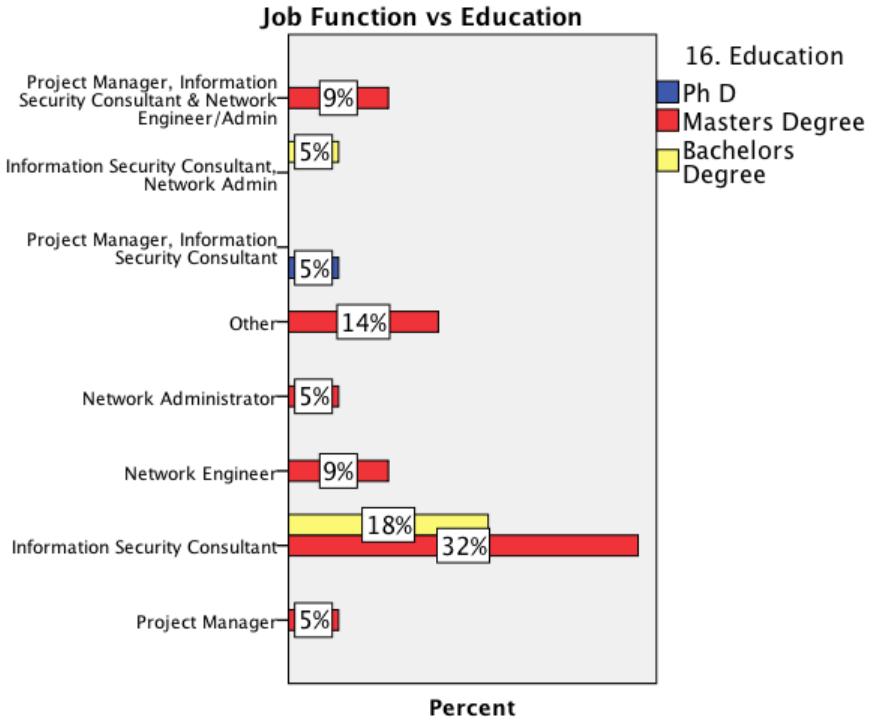

Figure 5.3 Respondent education and job function

5.2 Re-Classification of the Respondents

Figure 5.3 indicates that some respondents selected multiple job function classifications but for the analysis, the respondent job functions were reclassified from seven to the following four predominant groups: Information Security Contractor, Project Manager, Network Engineer/Administrator and Other. The priority for assignment of respondents that had multiple job classification was for them to be assigned in the following order: Information Security Contractor followed by Project Manager, Network Engineer/Administrator and then Other. The groups Network Engineer and Network Administrator were combined to form the group

titled Network Engineer/Administrator. The reduced group of four job function classifications ensured that the expected frequency value for the twenty-two respondents would not be less than five, as this provides erratic results for SPSS.

Four groups were selected as opposed to three or two groups because reviewing of the responses indicated the respondents could be categorized into one of the following four groups:

- Information Security Contractor
- Network Engineer/Administrator
- Project Manager
- Other

It is important to note that Network Engineers and Network Administrators perform all the tasks of Information Security Contractors but on a smaller scale (typically for just one organization or a subset of the enterprise). This relationship is discussed in Chapter 2 of the literature review. In Federal agencies and Federal Government contractors, Network Engineers and Network Administrators managing systems have to meet the annual security assessment requirements of FISMA.

Three of the respondents that classified themselves as 'Other' have job titles of Programmer, Systems Project Analyst and Contract Security Officer. The roles associated with these job titles are critical to the effective management of information assurance projects. Thus, the researcher could not justify excluding them from the research.

The responses were analyzed to determine if there is a statistical significance in the number of respondents for the four groups. The chi square test for the null hypothesis (H_0; the distribution of Information Security Contractors in the respondents for the data collection occurs with equal frequency) provided a (chi-square (3) = 22.364, $p<.01$). This means that the occurrence of the Information Security job function was significant for the population.

For the responses to the question of the respondent's expertise with entity relationship diagrams, a null hypothesis was developed stating "H_0: the distribution of respondents with expertise interpreting entity-relationship diagrams occurs with equal frequency". A significant deviation from the hypothesized values was found (chi-square (1) = 9.8, p<.01). The respondents were most likely to have expertise interpreting entity relationship diagrams.

Questions of the field questionnaire asked respondents to indicate their years of experience with Network Administration, Network Security, FISMA and Security Assessment. Figure 5.4 indicates that 81% of the respondents have four or more years of experience with Network Administration. Figure 5.5 indicates that the respondents that have four or more years of experience with Network Security were 81%. Figures 5.6 and 5.7 show that 59% of the respondents indicated that they had four or more years of experience with FISMA and Security Assessment. Next, we will examine the variation of the expertise of the respondents.

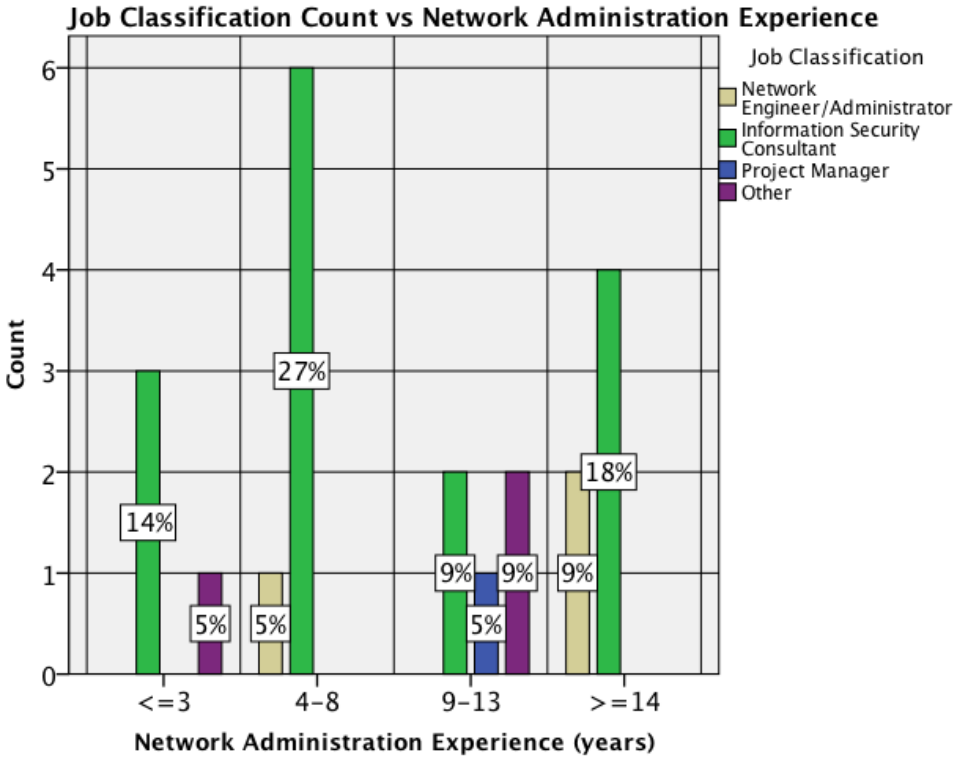

Figure 5.4 Job Classification Count vs. Network Administration Experience

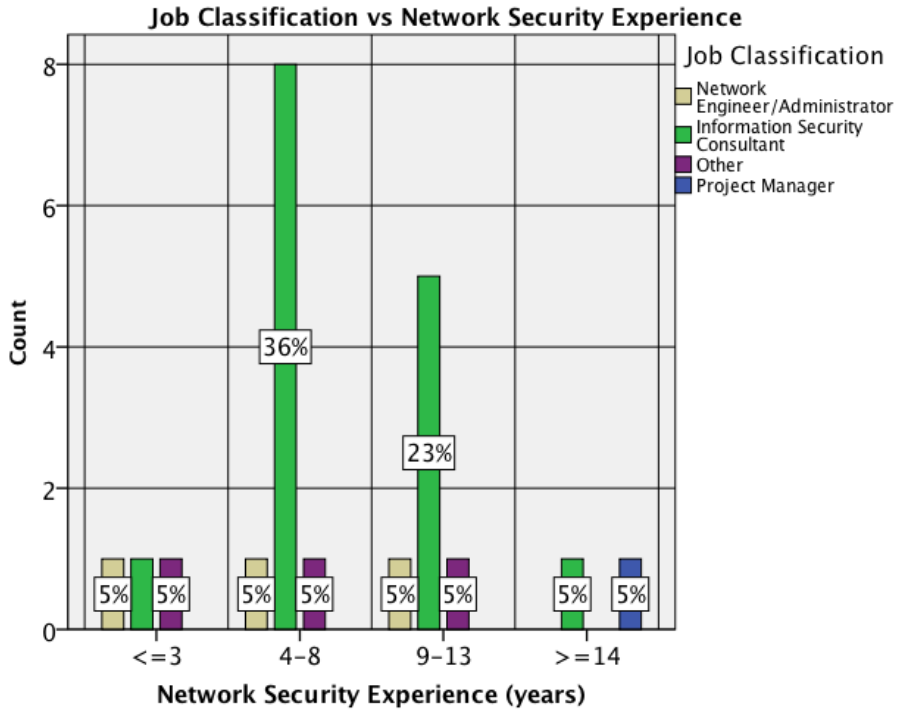

Figure 5.5 Job Classifications vs. Network Security Experience

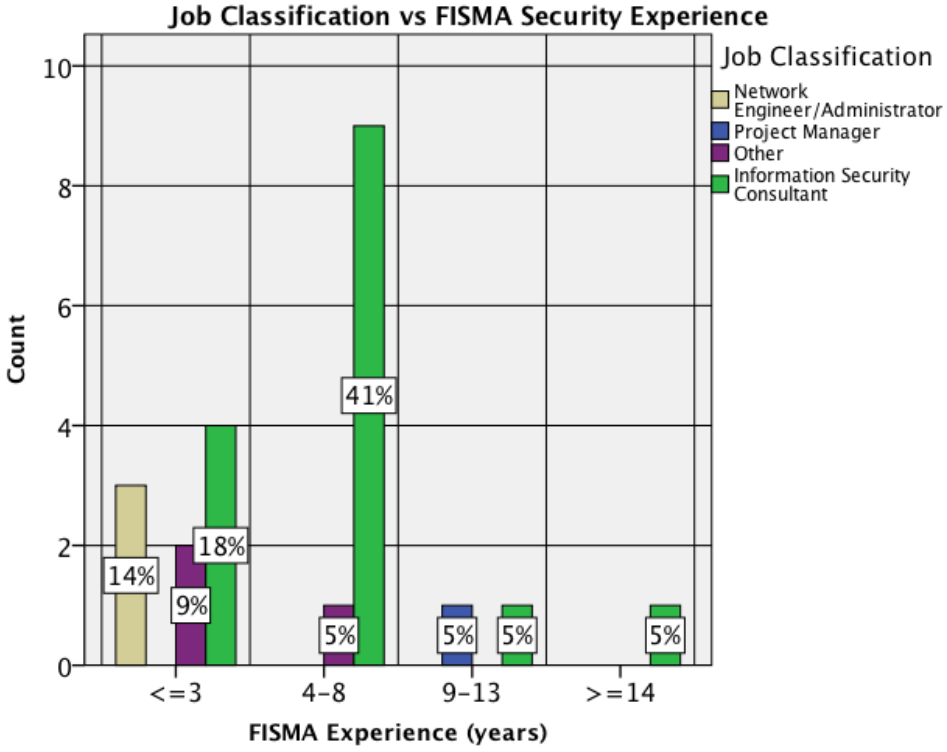

Figure 5.6 Job Classifications vs. FISMA Security Experience

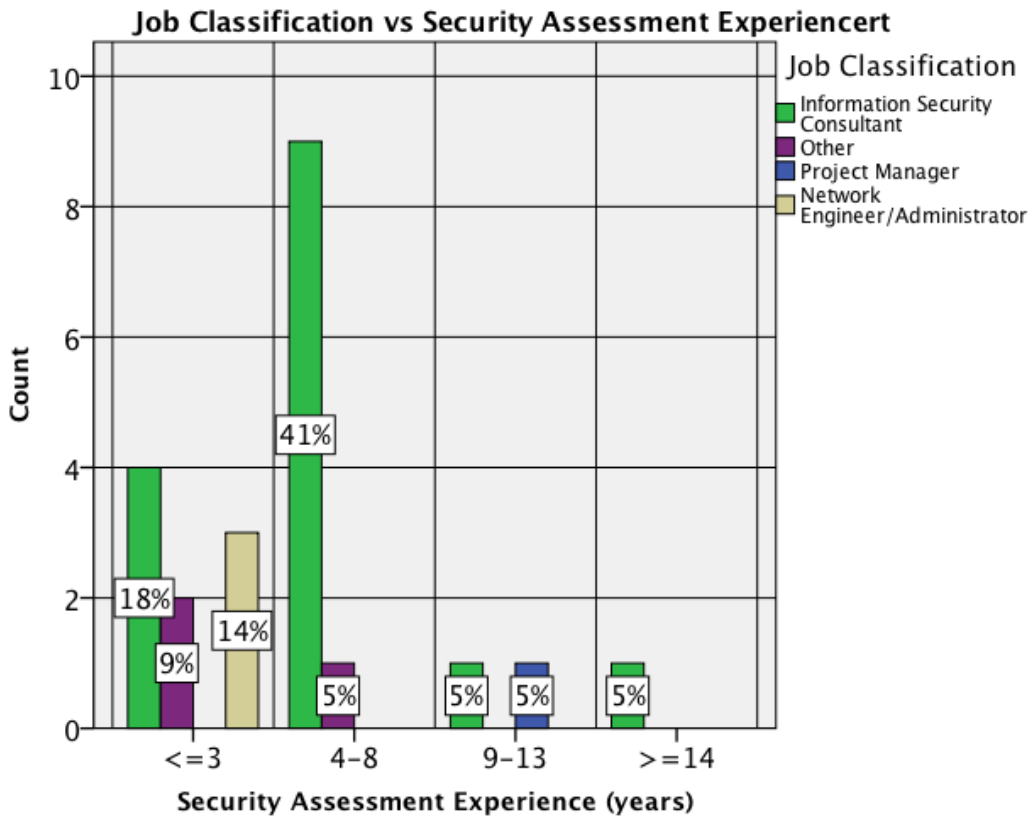

Figure 5.7 Job Classifications vs. Security Assessment Experience

Each of the four variables: Network Administration, Network Security, FISMA and Security Assessment were dichotomized into four dummy variables containing two groups. One group had three or less years of experience while the other group had four or more years of experience. Bivariate correlation was performed for the four dichotomized groups and a summary of the results is shown in Table 5.1. We note that there is a highly significant ($p<.01$) and a high correlations between the variables Dummy FISMA Experience and the Dummy Security Assessment Experience (0.812). The Dummy Security Assessment Variable and the Dummy FISMA Experience showed equal correlation (0.478) and significance ($p<0.05$) with the Dummy Network Security Experience. We also observed that the Dummy Network Administration Variable showed no significant correlation to the other three variables.

Table 5.1 Correlation for the Field of Experience of the Respondents

			Dummy Net. Sec. Exp.	Dummy Sec. Ass. Exp.	Dummy Net. Admin. Exp.	Dummy FISMA Exp.
Spearman's rho	Dummy Net. Sec. Exp.	Correlation Coefficient	1.000	.478*	.156	.478*
		Sig. (2-tailed)	.	.025	.488	.025
		N	22	22	22	22
	Dummy Sec. Ass. Exp.	Correlation Coefficient	.478*	1.000	-.153	.812**
		Sig. (2-tailed)	.025	.	.498	.000
		N	22	22	22	22
	Dummy Net. Admin. Exp.	Correlation Coefficient	.156	-.153	1.000	.087
		Sig. (2-tailed)	.488	.498	.	.700
		N	22	22	22	22
	Dummy FISMA Exp.	Correlation Coefficient	.478*	.812**	.087	1.000
		Sig. (2-tailed)	.025	.000	.700	.
		N	22	22	22	22

How do we explain all these correlations or lack thereof between the four levels of expertise of the respondents?

1. Network administrators do not typically perform the job functions of network security, FISMA and security assessments. This is the case because network administrators usually resolve problems related to computers and their associated users whereas network security job functions usually includes administration of the network infrastructure, that consists of switches, routers, Cisco PIX firewalls etc.
2. Experts who had job assignments related to implementation and management of FISMA requirements were also typically responsible for performing security assessments.
3. Network security experts sometimes had job assignments that involved FISMA and security assessment.

Table 5.2 shows the null hypothesis test results to determine if the respondents' years experience for network administration, network security, FISMA and security

assessments were significant. Based on the results we cannot reject the null hypothesis for the network administration and network security years of experience for the respondents. The FISMA and security assessments years of experience for the respondents reject the null hypothesis with four to eight years of experience being significant ($p<0.01$).

Table 5.2 Hypothesis Test for the Experience of the Respondents

Hypothesis Test Summary

	Null Hypothesis	Test	Sig.	Decision
1	The categories of 10. Net. Admin. Exp. occur with equal probabilities.	One-Sample Chi-Square Test	.823	Retain the null hypothesis.
2	The categories of 11. Net. Sec. Exp. occur with equal probabilities.	One-Sample Chi-Square Test	.059	Retain the null hypothesis.
3	The categories of 12. FISMA Exp. occur with equal probabilities.	One-Sample Chi-Square Test	.008	Reject the null hypothesis.
4	The categories of 13. Sec. Ass. Exp. occur with equal probabilities.	One-Sample Chi-Square Test	.008	Reject the null hypothesis.

Asymptotic significances are displayed. The significance level is .05.

5.3 Job function and Entity-Relationship Diagram Expertise

Of the twenty-two responses received only 20 answered the question on whether they had expertise with entity-relationship (E-R) diagrams. Figure 5.8 show three respondents (one from each job function category) had no experience with Entity Relation Diagrams. The remaining seventeen respondents had expertise with E-R Diagrams.

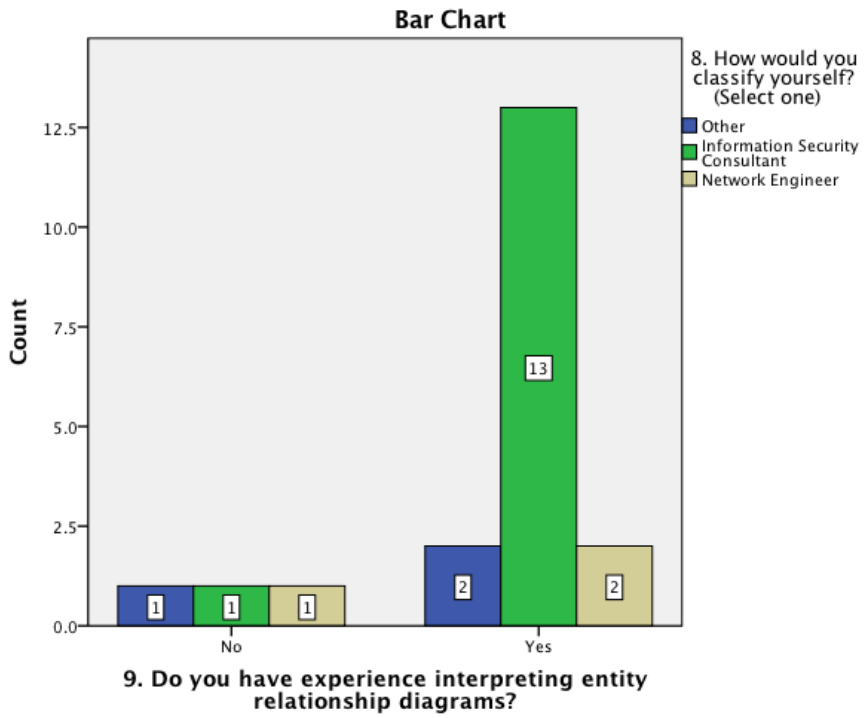

Figure 5.8 Respondent Experience with Entity-Relationship Diagrams

Statistically the respondents for the different job categories should balance out for the different categories of Information Security Contractor, Network Engineer and Other. A statistical comparison of responses for experience with E-R diagrams is depicted in Table 5.3. We observe that we can reject the null hypothesis and accept that the number of respondents with expertise interpreting E-R diagrams as significant at $p<0.01$. To alleviate the issue of respondents not having expertise with E-R diagrams, the interview items were worded so that respondents did not need to have any experience with E-R Diagrams to decide if they agree or disagree with a statement on the relationships between the different entities.

Table 5.3 Null Hypothesis Test for Experience with E-R Diagrams

Hypothesis Test Summary

	Null Hypothesis	Test	Sig.	Decision
1	The categories of 9. E-R Diag. Exp occur with equal probabilities.	One-Sample Chi-Square Test	.002	Reject the null hypothesis.

Asymptotic significances are displayed. The significance level is .05.

5.4 Surveyed Information Assurance Projects

This section discusses the characteristics of the information assurance projects completed by the respondents. Of the twenty-two respondents surveyed, two respondents did not answer the question on the number of information assurance projects completed. The total projects completed by the respondents is 432 with a mean of 21.6 projects and a standard deviation of 31.0. Three modes occurred at three projects, six projects and ten project points for the respondents.

There appears to be a discrepancy in the predominant number of years they have performed security assessment (3-8 years) and the number of projects for which the respondents have performed security assessment. Discussion with the respondents revealed that even though some of them have performed multiple security assessments, it was always for the same agency, so they counted the number of projects as one. I realized that given that my respondents had multiple years of experience with the same agency. A better question to ask would have been 'How many times have the respondents performed security assessments?' Given the confusion associated with this question, the metric of number of years performing security assessments is a better measure of the true expertise of the respondents.

Some of the Federal Government Agencies and organizations for which the respondents have performed security assessment include:

1. Department of Defense
2. Department of Homeland Security
3. Department of Education
4. United States Patent and Trademark Office
5. Federal Aviation Administration
6. Drug Enforcement Agency
7. Department of Health and Human Services
8. Department of Treasury
9. Center for Medicaid and Medicare Services
10. State of Florida
11. Environmental Protection Agency
12. Department of Labor
13. National Oceanic and Atmospheric Administration
14. General Service Administration
15. NASA
16. Executive Office of the President
17. US Capitol Police
18. Department of Interior (US Geological Survey)
19. US Department of Agriculture
20. Bank Of America

5.5 Analysis of Respondent Certifications

Of the twenty-two respondents, thirteen had industry-recognized certificates for information security or a related field. Eleven of the thirteen respondents holding industry recognized certificate also had Masters Degrees and the remaining two had Bachelor Degrees.

Table 5.4 shows the number and types of certificates held by the thirteen respondents and their degrees. Six of the respondents had the PMI PMP Certificate.

We must note that over half of the respondents had a Degree and an industry-recognized security certificate.

The biggest groups (50%) of respondents with industry-recognized certificates are Masters Degree holders with four to eight years of experience in the information assurance industry. This is reflected in the excellent feedback they provided on the survey questions and the models being validated.

Table 5.4 Respondent Certificate for the different degrees held.

		Education of the Respondents		
		Masters Degree	Bachelors Degree	Total
Certificates of the Respondents	CISSP	1	1	2
	CISSP, MCSE	1	0	1
	CISSP, PMP	0	1	1
	CISSP, PMP, GSNA, NASA-IAM	1	0	1
	CISSP, PMP, ITIL	1	0	1
	CISSP, PMP, NSA-IAM	1	0	1
	CISSP, Security+, ITIL	1	0	1
	MCSE	2	0	2
	MCSE, PMP, CCNA, CCNP	1	0	1
	MCSE, Security +	1	0	1
	PMP	1	0	1
Total		11	2	13

5.6 Information System Breakdown Structure Analysis

This section analyses the responses to questions from Section 2.0 of the data collection questionnaire that were intended to assess the value of the information systems breakdown structure that was developed as part of this research. The question assessed the following eight characteristics of the ISBS:

1. The sub-categories for the information system breakdown structure (Item 18)
2. The components for the computers sub-category (Item 19)
3. The components for the network infrastructure sub-category (Item 20)
4. The components for the personal digital assistant sub-category (Item 21)
5. The components for the imaging devices sub-category (Item 22)
6. The components for the other devices sub-category (Item 23)
7. The generic sub-components for the different components (Item 24)
8. The value of using the ISBS to identify organizational system assets (Item 25)

Eight positive summary statements were listed for the different characteristics and respondents were requested to indicate to what degree they agree with each statement using a four-point Likert scale that ranged from strongly disagree, disagree, agree and strongly agree. Scale ranking, recoding, chi-square test and nonparametric tests were performed on the responses. The procedure, findings and relevant discussions of the analyses follows.

5.7 Information System Breakdown Structure Scale Ranking

Table C17 in Appendix C shows the mean, mode and median values of the responses to Section 2.0 that contains items 18 to 25 of the data collection questionnaire. The mean ranges from 3.14 to 3.36 with a median and modal score of 3. The PDA Sub-Category had two sets of modes being 3 and 4. The values of using the ISBS had the highest score of 3.36 while the other sub-category had a value of 3.14. This implies that on average the respondents did agree with the statements provided in the questionnaire and believe that using an ISBS when performing security assessment is invaluable. Using a 4.0 mode to identify statements that the majority of the

respondents strongly agree with, we can say that a majority of the respondent strongly agree with the following statements for the ISBS:

1. The components identified for the personal digital assistants sub-category are sufficient to identify information systems for this sub-category
2. The components identified for the imaging devices sub-category are sufficient to identify information systems for this sub-category

The 'Other' sub-category had the lowest score of 3.14. This may be because it is the catchall for components that do not fit into the computers, network infrastructure, PDA or imaging devices sub-categories.

5.8 Information System Breakdown Structure Factor Analysis

The four categories of strongly disagree, disagree, agree and strongly agree were dichotomized into two groups named agree and disagree and a null hypothesis was develop for each of the statements and tested using Chi-square analysis to determine if there was significant difference between those who agreed and those who disagreed in the responses. The results of the Chi-square analysis are shown in Table C26 and the summary null Hypothesis table of the results is shown in Table 5.6. Based on the summary results, we can reject the null hypothesis at 99% ($p < 0.01$) confidence level and state that the number of respondents that agree with the positive statements of the information system breakdown structure are statistically significant compared to those that disagree.

Table 5.5 displays respondent feedback for the ISBS and the researcher's comments about the concerns/statements made by the respondent.

Table 5.5 Respondent Feedback and Researchers' Comments

#	Respondent Feedback	Researcher's Comments
1.	"I think the breakdown structure could cause confusion to some, but, if trained on properly, could be very useful. One of the biggest advantages I see is the assignment of responsibility. Determining system boundaries and ownership of data, system components, etc., is one of the most critical aspects of IT Security and C&A to me. So, I think a breakdown structure like this would greatly aid in defining those boundaries."	The use of a breakdown structure is not as common in the information security industry as it is in project management. Also the organizational breakdown structure can be matrix with the ISBS to assign responsibility for the different system boundaries. C&A stands for certification and accreditation, which is an internal process that organizations may perform to attest to the security posture of their systems. The CIO of the organization usually signs the C&A statement.
2.	"a fantastic representation that I could use as part of an assessment project. Very clever."	The purpose for developing the model for the ISBS.
3.	"Perhaps recognition of data (type of data) would be useful throughout that recognizes what may be stored or transmitted by a device."	The assessment of data that may be stored on the different information systems is outside the scope of this research. Other than for the network infrastructure, data tends to be organization-specific, so a generic classification of data will need a different assessment tool from that used in this research.

From some of the feedback and analysis conducted on the responses, we can see that there is a generally-expressed agreement on the usefulness of the ISBS and that coupling it with an assignment matrix would prove invaluable to some of the respondents. The assignment of responsibility for the different categories is typically

organization-specific as it depends on the size of the organization – See chapter 2. The use of the organizational breakdown structure is prevalent in project management and it is used to assign responsibility for tasks when matrixed with a work breakdown structure.

Table 5.6 Hypothesis Test Summary for the ISBS Model

Hypothesis Test Summary

	Null Hypothesis	Test	Sig.	Decision
1	The categories of Recode of ISBSFirstLevlCat to agree and disagree. occur with equal probabilities.	One-Sample Chi-Square Test	.001	Reject the null hypothesis.
2	The categories of Recode of ComputersSubCat to agree and disagree. occur with equal probabilities.	One-Sample Chi-Square Test	.003	Reject the null hypothesis.
3	The categories of Recode of InfrastructureSubCat to agree and disagree. occur with equal probabilities.	One-Sample Chi-Square Test	.000	Reject the null hypothesis.
4	The categories of Recode of PDASubCat to agree and disagree. occur with equal probabilities.	One-Sample Chi-Square Test	.003	Reject the null hypothesis.
5	The categories of Recode of ImagingSubCat to agree and disagree. occur with equal probabilities.	One-Sample Chi-Square Test	.003	Reject the null hypothesis.
6	The categories of Recode of OtherSubCat to agree and disagree. occur with equal probabilities.	One-Sample Chi-Square Test	.003	Reject the null hypothesis.
7	The categories of Recode of GenericComponents to agree and disagree. occur with equal probabilities.	One-Sample Chi-Square Test	.000	Reject the null hypothesis.
8	The categories of Recode of UseofISBS to agree and disagree. occur with equal probabilities.	One-Sample Chi-Square Test	.000	Reject the null hypothesis.

Asymptotic significances are displayed. The significance level is .05.

5.9 e-Government Relational Technical Controls Analysis

This section analyzes the responses to questions from Section 2.1 and contains items 27 to 50 of the data collection questionnaire. These items were developed to assess the relationships of the e-Government Relational Technical Control model that were developed as part of this research. The items assess the relationships between the following entities:

1. Users/Processes Entity and the Identification and Authentication (IA) Entity (Items 27 – 30)
2. System/Devices and the IA Entity (Items 32 – 35)
3. IA and Access Control (AC) Entity (Items 37 – 40)
4. AC and the Audit (AU) Entity (Items 42 – 45)
5. AU and the System and Communications Protection Entity (Items 47 – 50)

For each entity set, four statements were made about the relationships between the entities and the respondent was asked to indicate by selecting check boxes, to what degree they agree or disagree with the statements. A four-point Likert scale of strongly disagree, disagree, agree and strongly agree was used for the questionnaire. The respondents were provided with the option to provide feedback for any statements they strongly disagree or disagree with. Scale ranking, recoding, chi-square test and nonparametric tests were performed on the responses and the procedures, findings and relevant discussions of the analyses follows.

5.10 e-Government Relational Technical Controls Scale Ranking

Table C51 in Appendix C shows the mean, median and mode values of the responses to items 27 to 50 of the data collection questionnaire. The mean ranged from 3.05 to 3.77 with modal scores of 3's and 4's and median scores of 3, 3.5 and 4. Items 39, 43 and 45 were multi-modal with modes of 3 and 4. The relationship for item 27 that specifies that each user should have a unique identifier for authentication in an information system had the highest mean score of 3.77. The item with the least mean score of 3.05 was stating that an IA entity can exist that does not identify or

authenticate users/processes (i.e. it authenticates only systems and devices). These two items are opposing and appear to be on alternate sides of the mean. Using a 4.0 mode to identify statements that the majority of the respondents strongly agree with, we can say that the majority of the respondents strongly agree with the following statements for the e-Government Relational Technical Control E-R diagram:

1. Each User/Process should have a unique identifier for authentication in an information system
2. Users/Processes should be restricted to a single user/process id.
3. An IA entity should be capable of identification and authentication of multiple users/processes.
4. A system/device should have a unique identifier for authentication in an information system
5. An IA entity should be capable of identification and authentication of multiple systems/devices
6. Authenticated identifiers must be granted access to an information system
7. The access control entity should control the access of at least one authenticated identifier
8. The access control entity should be capable of managing the access of multiple authentication identifiers
9. The access control entity must create an audit event record
10. The access control entity may create multiple audit events
11. The audit and accountability entity must audit an access control entity
12. The audit and accountability entity may audit multiple access control entities
13. The audit and accountability entity should feed to a system and communications protection entity
14. The system and communications protection entity must monitor an audit entity

Another relationship that may be of interest to explore is that users may have multiple identifiers for the same information system. This was not performed in the research as we choose to assess the scale of zero-to-one instead of one-to-many. This

assessment can be performed in future research. Based on the mean, mode and median scores for all items on this section of the questionnaire being three or higher, we can say that on average the respondents were in agreement with the relationships expressed in the model.

5.11 e-Government Relational Technical Controls Factor Analysis

The four categories of strongly disagree, disagree, agree and strongly agree were dichotomized into two groups named agree and disagree and a null hypothesis was developed for each of the relationships between the entities and tested using Chi-square analysis to determine if there was significant difference between those who agreed and those who disagreed with the statements. The results of the Chi-square analysis are shown in Table C52. A summary null hypothesis table of the results is shown in Table C62 (in Appendix C). Based on the summary results we can reject the null hypothesis at 95% ($p < 0.05$) confidence level and state that the number of respondents that agree with the positive statements of the e-Government Relational Technical Control Model are statisitically significant.

Some of the dichotomized items converged on respondents' agreement with the statements and yielded a constant for which Chi-Square could not be calculated. Items that displayed a convergence for the responses include the following statements:

1. Each User/Process should have a unique identifier for authentication in an information system.
2. An IA entity should be capable of identification and authentication of multiple users/processes.
3. A System/Device should have a unique identifier for authentication in an information system.
4. An IA entity should be capable of identification and authentication of multiple systems/devices.
5. The access control entity should be capable of managing the access of multiple authenticated identifiers.

6. The access control entity must create an audit event record.
7. The access control entity may create multiple audit events.
8. The audit and accountability entity may audit multiple access control entities.

Table C64 (in Appendix C) displays respondent feedback for the relationships between the entities and the researcher's comments on the concerns/statements made by the respondent.

From the feedback, we see recommendations that explore the option for users to have multiple IDs based on their roles within the organization based on the different job functions they have to support. This item appears to be one of the issues that provided some of the most interesting feedback for the research.

5.12 Identification and Authentication Risk Management Analysis

This section analyses the responses to questions from Section 3 of the data collection questionnaire to assess the value of existing risk mitigation strategies that are based on the attributes of the identification and authentication entity. This analysis will identify those attributes that respondents believe are most effective in mitigating risks associated with the identification and authentication entity. The items in Section 3 analyzed the risk controls for the following seven identification and authentication attributes to determine which are effective and which should be discarded, modified or reconfigured for inclusion in the e-Government Relational Technical Controls E-R Diagram:

1. Identification and authentication of organizational users (IA-2)
2. Device identification and authentication (IA-3)
3. Identifier management (IA-4)
4. Authenticator management (IA-5)
5. Authenticator feedback (IA-6)
6. Cryptographic module authentication (IA-7)
7. Identification and authentication of non-organizational users (IA-8)

The first twenty-four items in the data collection covered statements related to the IA-2 to IA-5 security controls and asked the respondents to indicate to what degree they disagree or agree with each of the statements using a four-point Likert scale that ranged from strongly disagree, disagree, agree and strongly agree. The next two items were related to identifying durations for disabling user account and changing user passwords for IA-4 and IA-5 controls respectively. These were followed by five questions specific to the IA-5 control. The section closes with three items related to the IA-6, IA-7 and IA-8 families. All the questions were interspersed with the option for respondents to provide feedback on statements or questions they strongly disagree and disagree with.

Scale ranking, recoding, chi-square test and nonparametric tests were performed on the responses and the procedures, findings and relevant discussion of the analyses follows.

5.13 IA Risk Management Scale Ranking

The identification and authentication control family were analyzed for scale ranking and the detailed results are available in Tables C53 to C57 of Appendix C. A summary of those calculations is shows in Table 5.7. Questions on the Four-point Likert Scale had an average range of 3.05 to 3.68 for respondents that agreed with the statements provided. The lowest score of 3.05 was on the issues of using MAC addresses for identification and authentication of systems and devices while the highest score of 3.68 was on the need to uniquely identify users, processes, system and devices.

The lowest score for using MAC address for identification and authentication of system and devices is expected because hackers can spoof MAC addresses. The option of having systems and devices uniquely identified using other means is preferred over using the MAC address of the system. In addition, the requirement for users and processes having unique identifiers have been around in the information security industry long enough to have a convergence on this statement. The major

modal mark was three with select items showing multi-modal characteristics with 3 and 4 as the multi-modal marks.

Using a 4.0 mode to identify statements with which the majority of the respondents strongly agree. We can say that the majority of the respondents strongly agree with the following statements for the identification and authentication risk management strategy:

1. The identifier management and access control entities should be integrated for managing access to applications residing on the information system as well as the information system
2. The use of multi-factor authentication increases the security posture of information systems
3. Having one of the factors of multi-factor authentication provided by a device separate from the information system accessed improves the security posture of the information system
4. Users, processes, systems and devices must be uniquely identified to an information system
5. Limiting the reuse of authenticators for users/processes improves the security posture of information systems
6. The used of automated tools to determine the strength of authenticators to resist attacks improves the security posture of information systems
7. Employing the use of single sign-on improves the security posture of information systems
8. The use of cryptographic modules during authentication improves the security posture of information systems
9. The period of inactivity before a user account is disabled should be 61 to 90 days
10. Authenticators (or passwords) should be changed/refreshed every 61 to 90 days
11. Information systems should remember and prevent users from using 4-6 password histories

12. The minimum password characters should be between eight and ten characters
13. Security authenticators should be capable of the following characteristics
    a. Ensuring passwords are case sensitive
    b. Exceed a certain number of characters
    c. Including both upper and lower case letters
    d. Requiring the use of numbers
    e. Requiring the use of special characters
    f. Having a minimum requirement set for passwords

Table 5.7 Summary of the IA Risk Management Scale Ranking Results

#	Control ID	Question Type	Range of Means	Modes
1.	IA-2	Four-point Likert Scale (Items 52-58)	3.36 – 3.5	3
2.	IA-3	Four-point Likert Scale (Items 60 – 63)	3.05 – 3.45	3
3.	IA-4	Four-point Likert Scale (Items 65 – 68)	3.23 – 3.68	3 & 4
4.	IA-5	Four-point Likert Scale (Items 70 – 78)	3.05 – 3.55	3 & 4
5.	IA – 4/5	Five-point Ordinal Scale (Items 79 & 80)	2.64 – 2.68 (different scale)	3
6.	IA-5	Four-point & Five-point Ordinal Scale (Items 81 & 82)	2.23 – 2.27 (different scale)	2
7.	IA-5	Yes/No Nominal Scale (Item 83)	0.68 – 1 (different scale)	1
8.	IA-6	Four-point Likert Scale (Item 85)	3.41	3
9.	IA-7	Four-point Likert Scale (Item 86)	3.64	4
10.	IA-8	Four-point Likert Scale (Item 87)	3.32	3

5.14 IA Risk Management Factor Analysis

The items that used a four point Likert scale were dichotomized into two groups of agree and disagree. A null hypothesis was developed for the dichotomized variables and then tested using Chi-square and Binomial tests to determine if there was significant difference between those who agree and disagree in the responses. The results of the tests are shown in Table C58. The following risk management strategies for the identification and authentication control family received the approval of all respondents and indicated a convergence of knowledge for the following industry best practices:

- The identification and authentication control family should be used to manage identifier generators for an information system.
- The identifier management and the access control entities should be integrated for managing access to applications (residing on the information system) and the information system
- Authenticators should make use of time synchronous or challenge-response one-time authenticators
- Authenticators should use bidirectional authentication between devices
- Users, processes, systems and devices must be uniquely identified to an information system
- User identifiers should be disabled for an organization-defined period of inactivity (the range was 61 – 90 days)
- Identifier generators should limit the reuse of authenticators for users & processes
- Organizations must establish and implement a maximum period before requiring a password change (the recommended period was found to be 61 to 90 days)
- When logging on to the information system, feedback during authentication should be obscured

The dichotomized questionnaire item 76 that relates to the use of single sign-on is not significant at the 95% ($p < 0.05$) confidence level. Table C65 (in Appendix C) depicts the results of hypothesis tests performed on the dichotomized variables that were not constant.

Based on the results of the Chi-Square and Binomial Tests we can state that at the 99% confidence level we can make the following statements for the identification and authentication control risk management strategies that effectively improve the security posture of information systems:

1. Authenticated user/process IDs should be granted access to the information system
2. Use of multi-factor authentication for information systems
3. Identifier generators should be capable of multi-factor authentication
4. Have one of the factors of multi-factor authentication provided by a device separate from the information system being accessed
5. System/device IDs should be centrally managed by an information system
6. Use IP addresses for identification and authentication of devices and systems
7. Prevent the reuse of user, process, system or device identifiers
8. Employ user identifiers that do not match the email address of users
9. Limit the reuse of authenticators for users and processes
10. Establish a minimum period before requiring a password change
11. Use automated tools to determine the strength of authenticators to resist attacks
12. Use unique authenticators (or passwords) for different information systems
13. Use one-time passwords
14. Restrict the number of accounts individuals have on multiple information systems
15. The duration before authenticators are changed should be in the range of sixty one to ninety days.
16. The minimum number of characters for passwords should be between eight and ten characters
17. Password authenticators should be case sensitive
18. Passwords should consist of upper and lower case letters
19. Passwords should consist of special characters
20. Passwords should be obscured when they are being entered

21. Non organizational users of the system should be authenticated to information systems

At the 95% confidence level, we can make the following statement about factors that improve the security posture of information systems for the identification and authentication control risk management:

1. Use MAC address for identification and authentication of devices and systems

Some of the salient feedback received from the respondents for this section of the questionnaire is discussed in Table C66.

5.15 User/Process Entity & IA Attributes Association/Correlation

The user/process entity and the identification and authentication risk management strategies were assessed to identify any association or correlation. The results of the association and correlation tests for the variables are documented in the cross cells for the two variables of Table C67 (in Appendix C). The Somers'd and Gamma values and their corresponding significance were calculated to establish associations where as the Spearman rho was calculated to establish a correlation between the variables. The cells highlighted in yellow cells show the variables that were significantly associated and correlated, while the pink cells show those that are significantly associated without any significant correlations. These values further validated the relationships between the user/process entity and its corresponding risk management strategies.

5.16 System/Device Entity & IA Attributes Association/Correlation

The system/device entity and the identification and authentication risk management strategies were assessed to identify any association or correlation. The results of the association and correlations tests for the variables are documented in the cross cells for the two variables of Table C68. The Somers'd and Gamma values and their corresponding significance were calculated to establish associations where as the

Spearman rho was calculated to establish a correlation between the variables. The cells highlighted in yellow cells show the variables that were significantly associated and correlated, while the pink cells show those that are significantly associated but without any significant correlations. These values further validated the relationships between the system/devices entity and its corresponding risk management strategies.

5.17 IA Security Assessment Cost Calculations Assumptions

The following assumptions were made for the development of the cost model for the security assessment of the identification and authentication control family:

1. The maximum duration for performing the different tasks for the assessments is eight hours.
2. When calculating the duration for performing the different tasks, we will use the upper limits for the tasks to get conservative estimates.
3. The probabilities for the contributions of the different tasks shall be based on the frequency they were selected by the respondents.
4. The organization allows invoicing in tenths of an hour.
   The duration for performing these tasks and their corresponding probabilities are shown in tables 5.8, 5.9, 5.10 and 5.11.

5.18 IA Security Assessment Cost Model Analysis

In this section, we will determine how much to bid on a project to assess the identification and authentication control, given that the tasks involved include:

1. Assessment of identification and authentication documents
2. Interviews of the pertinent IA organizational stakeholders
3. Testing of the identification and authentication controls in place
4. Development of a report on the identification and authentication control

Table 5.8 Duration & Probabilities for Assessing the IA Security Documents

		Frequency	Valid Percent	Cumulative Percent
Valid	<=1	1	5.0	5.0
	2-3	7	35.0	40.0
	4-5	4	20.0	60.0
	6-7	3	15.0	75.0
	>=8	5	25.0	100.0
	Total	20	100.0	

Table 5.9 Duration & probability for conducting interviews of IA personnel

		Frequency	Valid Percent	Cumulative Percent
Valid	<=1	3	15.0	15.0
	2-3	6	30.0	45.0
	4-5	4	20.0	65.0
	6-7	7	35.0	100.0
	Total	20	100.0	

Table 5.10 Duration and probabilities for testing of the IA security controls

		Frequency	Valid Percent	Cumulative Percent
Valid	<=1	3	15.0	15.0
	2-3	7	35.0	50.0
	4-5	4	20.0	70.0
	6-7	5	25.0	95.0
	>=8	1	5.0	100.0
	Total	20	100.0	

Table 5.11 Duration and probabilities for developing the IA security reports

		Frequency	Valid Percent	Cumulative Percent
Valid	<=1	1	5.0	5.0
	2-3	4	20.0	25.0
	4-5	5	25.0	50.0
	6-7	6	30.0	80.0
	>=8	4	20.0	100.0
	Total	20	100.0	

The duration ranges (in hours) for security assessment of the IA controls consist of the following:

- <=1
- 2-3
- 4-5
- 6-7
- >=8

We want to determine if the respondents who answered eight hours or greater is significant, so we dichotomize the ranges into two groups consisting of the following:

- Group 1 (<=1, 2-3, 4-5 an 6-7)
- Group 2 (>=9)

A test of the null hypothesis shows that the Group 1 items are significant at the 95% confidence to reject the null hypothesis. The calculations for the Chi-Square test and the null hypothesis are show in Table 5.12 and Table 5.13 respectively.

Table 5.12 Chi-Square Test for a different between Group 1 and Group 2

	D89 Duration to assess IA documents	D91 Duration to test IA controls	D92 Duration to develop IA report
Chi-square	5.000[a]	16.200[a]	6.368[b]
df	1	1	1
Asymp. Sig.	.025	.000	.012

a. 0 cells (.0%) have expected frequencies less than 5. The minimum expected cell frequency is 10.0.

b. 0 cells (.0%) have expected frequencies less than 5. The minimum expected cell frequency is 9.5.

Table 5.13 Hypothesis Tests for significance between Groups 1 & 2

Hypothesis Test Summary

	Null Hypothesis	Test	Sig.	Decision
1	The categories defined by D89 Duration to assess IA documents = 2 and 1 occur with probabilities 0.5 and 0.5.	One-Sample Binomial Test	.041[1]	Reject the null hypothesis.
2	The categories defined by D91 Duration to test IA controls = 2 and 1 occur with probabilities 0.5 and 0.5.	One-Sample Binomial Test	.000[1]	Reject the null hypothesis.
3	The categories defined by D92 Duration to develop IA report = 1 and 2 occur with probabilities 0.5 and 0.5.	One-Sample Binomial Test	.019[1]	Reject the null hypothesis.

Asymptotic significances are displayed. The significance level is .05.

[1] Exact significance is displayed for this test.

Table C60 shows a Bayesian probability calculation based for the duration of the different tasks for a maximum, minimum and median is with the maximum durations as follows:

- IA Document assessments (5.2 hrs)
- IA Interview of the stakeholders (4.5 hrs)
- IA Control Tests (4.4 hrs)
- IA Report Development (5.6)

Most of the respondents chose not to provide this data and those that did provide this data provided an hourly rates range of $35/hr to $250/hr. We observe the large variation because the pilot test was not worded properly so some respondents were providing their individual pay rate instead of the rate their organizations charge for security assessments.

The hourly rates charge by organizations is approximately $125/hr. This was obtained from speaking with industry experts and looking up the GSA schedule rate for hourly billing of information security contractors. The rate could range from $125/hr to $250/hr depending on the level of expertise, credentials and skill set of the information security contractor.

The consensus from respondents was that the average is somewhere around $125/hour. We note that the median cost of performing security assessment for the identification and authentication control family is:

Sum of the hours for all tasks * hourly rate = (5.2 + 4.5 + 4.4 + 5.6) * 125 = $2,462.50

Chapter 6: Baldrige National Quality Program Case Study

6.1 Data Collection and Reliability of the Case Study

The data collection for the case study addressed the issue of reliability by triangulation. The researcher reviewed the case study documentation, conducted an informal interview with pertinent personnel and then developed a report that was discussed with pertinent personnel to validate the contents of the report.

6.2 Baldrige National Quality Program Case Study

Background

The Malcolm Baldrige National Quality Award is one of the highest recognition that a US organization may achieve. The goal of this award is to increase US businesses competitiveness in the global market place and ensure the economic security of US organizations. Traditionally, the award is presented annually by the President of the United States to organizations that have excelled in the quality of their products or services.

President Ronald Reagan made this comment about the award program: “America’s economic strength depends on industry’s ability to improve productivity and quality and to remain on the cutting edge of technology, and that’s why the Malcolm Baldrige National Quality Award is so important.” Other presidents, including George H. W. Bush, William J. Clinton and George W. Bush have shared similar sentiments. The typical areas that the award covers include business, education, health care and nonprofit organizations. It is important that we note that these organizations cannot have economic security without having secure information systems.

The National Institute of Standards and Technology manages the Baldrige National Quality Program. Recipients of this award are required to share information on their

successful performance and quality strategies with other US organizations at the annual Quest for Excellence Conference. The rigorous process of applying for the award helps organizations align their processes and resources with their organizational goals and objectives. It also helps organizations engage their workforce and customers in continuous improvement dialogue. At the end of the assessment, organizations that apply for the award are provided with a detailed feedback report based on evaluation of their organization by specially trained experts.

The seven categories against which organizations are assessed include the following:

- Leadership
- Strategic Planning
- Customer Focus
- Measurement, Analysis and Knowledge Management
- Workforce Focus
- Process Management
- Results

Of the seven categories, the Measurement, Analysis and Knowledge Management category is of the most interest to this research. The category of Measurement, Analysis and Knowledge Management contains the sub-category of Management of Information, Knowledge and Information Technology, which is the subject of this case study. The sub-category has 45 points of the total 1000 points for the entire assessment. This sub-category assesses how organizations manage information, organizational knowledge and information technology.

Management of Information, Knowledge and Information Technology

The primary task for the Management of Information, Knowledge and Information Technology is twofold and worded as follows:

1. Describe HOW your organizations ensure the quality and availability of needed data, information, software, and hardware for your WORKFORCE, suppliers, PARTNERS, COLLABORATORS, and CUSTOMERS
2. Describe HOW your organization builds and manages its KNOWLEDGE ASSETS.

Guidelines for answering these two questions call for applicants to provide evidence that relates to these areas:

a. Data, Information, and Knowledge Management and;
b. Management of Information Resources and Technology

Data, Information and Knowledge Management

This area requires applicants to delineate how they ensure their organizational data, information and knowledge is accurate, timely, available and accessible to their stakeholders while meeting the requirements for integrity, reliability, security and confidentiality. It also calls for organizations to highlight how they collect and transfer knowledge to pertinent stakeholders, rapidly identify, share and implement best practices that support the organization's strategic goals.

Management of Information Resources and Technology

This area calls for organizations to explain how they ensure that hardware and software are reliable, secure and user-friendly. It also looks at the business continuity plans of organizations and their strategic plans for maintaining a competitive advantage on information technology.

6.3 Baldrige National Quality Program - Research Application

The Management of Information, Knowledge and Technology sub-category calls for organizations to delineate how they ensure the confidentiality, availability and integrity of their data, information and information technology resources. This call is consistent with the FISMA requirements and the goal of the NIST SP 800 series

documents. We can argue that this convergence in requirements is partly due to NIST being responsible for the successful implementation of both programs for organizations. The two programs may be affected by a concentration of knowledge.

The e-Government Relational Technical Controls Taxonomy that is comprises of the ISBS model and the e-Government Relational Technical Controls Model could help organizations meet the requirements of the Baldrige National Quality Program by helping them:

- Identify hardware and their related software resources by documenting them in the ISBS
- Depict how hardware and software are managed by developing a responsibility assignment that consists of a matrix between the organizational breakdown structure and the ISBS
- Depict the source and destination of data/information that is shared between the organization and its pertinent stakeholders
- Utilize the ISBS to identify the location of data and information stored on the resources and their corresponding security classifications
- Utilize the ISBS to show the partitioning and mappings of their operations environment to their backup site and how the organization ensures business continuity
- Manage the confidentiality, availability and integrity risk of their data, information and information systems

The Management of Information, Knowledge and Information Technology has direct relevance to the e-Government Relational Technical Controls Taxonomy. This taxonomy can help organizations better understand their information technology infrastructure vis-à-vis the requirements for the Malcolm National Quality Program.

Chapter 7 Conclusions and Recommendations

This chapter discusses the methodology used in formulating the research, summarizes the key findings and addresses the research limitations and recommendations for future work.

7.0 Research Summary

This section discusses the summary of the findings of the research. FISMA and the use of the NIST SP 800-53 Rev 3, has improved the way organizations practice information assurance. The NIST SP 800-53 has limitations that result in the following issues:

1. Fifteen security controls were withdrawn from the NIST SP 800-53 Rev 3 released in August 2009
2. The security controls are documented in a generic format that is not specific to any particular information systems. This often results in security assessment teams addressing controls that only apply to email servers to routers when performing security assessments. The controls have not been customized for the information system landscape.
3. There is a waste of resources (time and money) associated with performing security assessments using the hierarchical structure of the NIST SP 800-53, which is not specific to an information system
4. There is no real-time tool that can be used to identify information systems and map the assignment of responsibility to the associated information systems and data stored on the systems
5. There is no documented evidence that the knowledge base of information security contractors has been surveyed to assess the value of the identification and authentication security controls in mitigating risks to an organizational information system.

Often when project managers consider risks to a project, they only consider risks associated with schedule delays, cost, customer satisfaction and quality. Rarely do

they consider risks associated with information systems. The literature review indicates that these risks are real and can significantly affect the success of a project. Project environments are pervaded with information systems that facilitate communication, reporting and collaboration between teams. The literature indicates that risks associated with the use of information systems should be addressed, or else their likelihood of derailing a project increases.

The research was conducted to answer the following questions:

1. Can we develop an e-Government Technical Controls Relational taxonomy for Federal Government Information Assurance Contractors?
2. What are some effective risk mitigation and management strategies for the Identification and Authentication Security Control Family?
3. What are the associated cost calculations for performing security assessment of the Identification and Authentication Security Control Family?

This research developed a ISBS model that can be used for identification of information system resources for a project or organization while providing a relational approach to security assessments. e-Government Relational Technical Security Controls model entity-relationship and positive risk management statements for the identification and authentication control family were developed. The e-Government Relational Technical Controls model is an entity relationship diagram that is comprised of entities, their attributes and the relationships between them. To alleviate the likelihood of "garbage-in garbage-out", there was a need to validate the attributes of the identification and authentication control family to identify effective risk mitigation and management strategies.

The researcher also developed a cost model for establishing the baseline cost of performing security assessment for the identification and authentication control family. This results in reduced time and cost savings when performing security assessments as the controls that are not applicable to an information system will not

be addressed. In addition, risk mitigation and management strategies for the identification and authentication control family are assessed.

7.1 Information System Breakdown Structure Model Conclusion

A comprehensive literature review was performed coupled with several unstructured interviews of information security contractors to identify some of the challenges plaguing Federal information assurance contractors. Based on the information obtained, a model for an information system breakdown structure (ISBS) model.

The ISBS model is hierarchical and composed of a category, sub-categories, components and sub-components. The ISBS can be further decomposed to the module and the sub-module levels but this level or decomposition is outside the scope of the research.

The models and statements developed were documented in a questionnaire that resulted in twenty-two responses from information security experts and other security practitioners. The research findings recommend that the ISBS should be considered a living tool and should be customized for a project or organization with the goal of identifying and managing sources of project information system risks.

The ISBS can be matrixed with the project WBS to identify which information systems are required for successfully completing the tasks. This is especially important for managing risks associated with tasks that are on the critical path and heavily dependent on information systems. After identifying the most critical information system resources and those that are required for tasks on the critical path, the ISBS should be used as a collaborative tool to identify suitable risk management strategies for the affected information system.

The risk mitigation and management strategies can be used to develop a backup plan, a business continuity plan or a contingency and disaster recovery plan at the

organizational level. Information system resources that do not have a backup plan and are not included in the business continuity plan or the disaster recovery plan should, have information system risk mitigation and management plan develop at the project level.

Feedback received during the validation of the ISBS model stated, "One of the biggest advantages I see is the assignment of responsibility. Determining system boundaries and ownership of data, system components, etc is one of the most critical aspects of IT Security and C&A to me. So, I think a breakdown structure like this would greatly aid in defining those boundaries." This feedback indicates that the ISBS could also be used for assigning project responsibility when performing security assessments. This is accomplished by creating a matrix of the ISBS and the project organizational breakdown structure. Organizations may choose to use the ISBS to assign responsibility for organizational information systems. Depending on the level of criticality of the project, a scorecard could be developed to track the health of critical project and organizational information systems.

One of the first steps when performing security categorizations is to determine the Federal Information Processing Standards (FIPS) 199 security categorization of the systems. The FIPS 199 security categorization involves classifying the security of the information system into a high, moderate or low category. This determines the type and amount of security controls that must be applied to a system. The ISBS can be used to perform FIPS 199 security classification of information systems and to evaluate how the categorization of one system may affect other systems and the best way to partition systems based on their security categorizations. Different ISBSs can be developed based on the security categorizations of the systems.

Another feedback that leads to the identification of an alternative use of the ISBS is "Perhaps recognition of data (type of data) would be useful throughout that recognizes what may be stored or transmitted by a device." The ISBS can be used as a basis for the development of a data structure that maps to the different information

systems in use on a project or by an organization with the goal of determining not only their security categorization but also for the development of business continuity and backup plans. Another option would be to develop a data breakdown structure that maps to the ISBS and depicts data in situ.

The research analysis and results supported the development of this model and validated its usefulness to information security contractors. A final feedback that emphasized the value of the ISBS model includes “a fantastic representation that I could use as part of an assessment project. Very clever.”

7.2 e – Government Relational Technical Controls Model Conclusion

The information system breakdown structure (ISBS) was incorporated into the e-Government Relational Technical Controls. The e-Government Technical Controls Model is an entity relationship diagram developed using the security controls of the NIST SP 800-53 Rev 3 Technical controls and entities for users/process and system/devices. The relationship between the entities is represented by the cardinalities of one-to-many and zero-to-many. The e-Government Relational Technical Controls provide the opportunity to map security controls to their applicable user, process or information system.

Items in the questionnaire addressed the five relationships between the entities. Based on the analysis of the results of the questionnaire, the relationships developed appeared to be sufficient for the e-Government Technical Controls. Some of the feedback received from the respondents suggests that the relationship between the IA Entity and the Users/Processes and the Systems/Devices should be represented by a one-to-many relationship instead of a one-to-one relationship.

A one-to-one relationship means that a user should have only a single user identifier, as is typically implemented with single-sign-on. Single-sign-on allows a user to sign on once and track/manage their access to all resources on the network. This reduces administrative overhead and the likelihood of users writing down their passwords and keeping them around their work area.

The use of multiple passwords for multiple information systems improves logical security but the need for users to remember multiple passwords may result in them writing the passwords on sticky notes around their work area. Another options proposed is the used of one-time password tokens for the different information systems while the user maintains a single identifier and password. This method will provide the benefit of having multiple passwords for multiple systems but the user only has to remember a single password and identifier.

Another major improvement in using the e-Government Relational Technical Controls is that the likelihood of having duplicate controls will be reduced as the different attributes for the entities can be related to each other. This model also presents a more integrated approach to the handling of security as opposed to the hierarchical approach.

7.3 Identification and Authentication Risk Management Conclusion

The attributes for the identification and authentication control family were assessed for their ability to mitigate and manage risks to entities identified in the information systems breakdown structure. The risk management strategy that was ranked the lowest was the use of MAC addresses for identification of information systems. Respondent feedback, and the information security body of knowledge indicates that MAC addresses can be spoofed, supported this ranking.

The risk mitigation strategy with the highest ranking is that each user should be uniquely identified to the information system. This improves the non-repudiation of user actions and improves the chances of their actions to be admissible in court, though it is still considered hearsay. Some other pertinent risk mitigation and management strategies identified for information systems include:

1. Using multi-factor authentication for information systems
2. IA entities generators should be capable of multi-factor authentication
3. Having one of the factors of multi-factor authentication provided by a device separate from the information system being accessed
4. System/device IDs should be centrally managed by an information system
5. Using IP and MAC addresses for identification and authentication of devices and systems
6. Preventing the reuse of user, process, system and device identifiers
7. Employing user identifiers that do not match the email addresses
8. Restricting the reuse of authenticators for users and processes
9. Establishing a minimum period before requiring a password change

10. Using automated tools to determine the strength of authenticators to resist attacks
11. Using unique authenticators (or passwords) for different information systems
12. Using tokens that offer one-time passwords
13. Restricting the number of accounts individuals have on multiple information systems
14. Ensuring that the duration before authenticators are changed is in the range of sixty one to ninety days.
15. Ensuring that the minimum number of characters for passwords should be between eight and ten characters
16. Ensuring that password authenticators are case sensitive
17. Ensuring that passwords consist of upper and lower case letters
18. Ensuring that passwords contain of special characters
19. Protecting users from "shoulder surfing"
20. Ensuring that non-organizational users be authenticated to the information systems

7.4 Recommendations for Future Work

Although this research has made theoretical and practical contributions to project management as it relates to mitigating project risks associated with the use of information systems. There is an extensive amount of research available for future work that cannot be covered in this research. Some of such research includes:

- Developing a data classification tool that maps to the information system breakdown structure
- Validating the Access Control, Audit, and Systems and Communications Protection attributes from the e-Government Relational Technical Control Model for risk management.
- Identifying effective risk mitigation and management strategies for the Access Control, Audit, and Systems and Communications Protection
- Developing and validating a model for the e-Government Management controls

- Developing and validating a model for the e-Government Operational controls
- Developing and validating a risk mitigation and management model
- Investigating the possibility of integrating all three models (technical, operation and management) into one so that they provide a fully-integrated approach to information system security

Appendix A: Data Collection Questionnaire

e-Government Relational Technical Controls Data Collection

Dear Sir/Madam,

Based on your recognized expertise in information systems security you are kindly requested to participate in the **University of Maryland** research requiring data collection related to e-Government Relational Technical Controls. In our data collection effort, we ask information security industry experts such as yourself questions about the integration of the Identification and Authentication Control for the NIST SP 800-53 Rev 3 within information system(s) and assess the value of a relational model and an information system breakdown structure for performing security assessments. This data collection will require completion of this questionnaire.

Of course, your participation in this research effort is voluntary and the time taken from your busy schedule will be much appreciated. There are no foreseeable risks associated with this project. However, if you feel uncomfortable answering any questions, you can withdraw from the data collection exercise at any point. It is very important for us to learn your opinions on this subject.

Your responses will be strictly confidential and data from this research will be reported only in an aggregate form. If you have questions at any time about our data collection or the procedures, you may contact the project supervisor at the University of Maryland, College Park, Dr. M. Skibniewski at 301-405-9364 or by email (preferred) at mirek@umd.edu.

Yours sincerely,

Momodu Fofana, PhD C, MIS, B. Eng, PMP, CISSP, CCNA
Research Associate

Email: mfofana@umd.edu
Phone: (240) 533-6757

Section 1

Section 1.0 Respondent Information

In this section, I will collect your personal information. We are requesting your email address so we can send you a copy of the results of the data assessment effort. We shall not include your email in any of our mailing lists or send you any additional information besides that directly related to this research. The additional information requested may be use as a basis for comparison of your responses to those of other respondents.

1. Date:	2. Location:
3. Name:	4. Title:
5: Telephone #:	6: Email:
7. Interviewer:	
8. How would you classify yourself? (Select all that apply) ☐ Project Manager	9. Do you have experience interpreting entity relationship diagrams?

☐ Information Security Contractor ☐ Network Engineer ☐ Network Administrator ☐ Other:	

10. Years of experience in the network administrator related field (Select one)

☐ <= 3

☐ 4 - 8

☐ 9 - 13

☐ >= 14

11. Years experience in the network security related field (Select one)

☐ <= 3

☐ 4 - 8

☐ 9 - 13

☐ >= 14

12. Years experience in the FISMA e-Government implementation related field (years)

☐ <= 3

- [ ] 4 - 8
- [ ] 9 - 13
- [ ] >= 14

13. Years experience in performing security assessments using the NIST Control Families (Select one)

- [ ] <= 3
- [ ] 4 -8
- [ ] 9 - 13
- [ ] >= 14

14. Experience in performing security assessments using the NIST Security Control Families (in years)

15. How many projects involving security assessments have you worked on?

16. Select the industry recognized certificates you hold.

- [ ] CISSP

- ☐ MCSE
- ☐ PMP
- ☐ CSA
- ☐ None
- ☐ Other:

16-i. What is your highest level of education? (Select all that apply)

- ☐ High School Diploma
- ☐ Associate Degree
- ☐ Bachelors Degree
- ☐ Masters Degree
- ☐ PhD
- ☐ Post Graduate
- ☐ Other

Additional Information Systems Security Information

17. What is your highest level of education? (Select all that apply)

End of Section 1

Section 2

Section 2 marks the start of the research data collection.

Section 2.0Information Systems Breakdown Structure Validation

This section establishes the value of using an Information Systems Breakdowns Structure to identify and classify the organizational information system resources that may be utilize on a project. Figure 1.0 depicts the category as information system breakdown structure and the following sub-categories: Computers, network infrastructures, personal digital assistants, imaging devices and other devices. Figure 1 also highlights the components and sub-components for each sub-category. The following interview items assess the importance of using an information system breakdowns structure to identify the information systems assets whose risks should be identify, mitigate and manage.

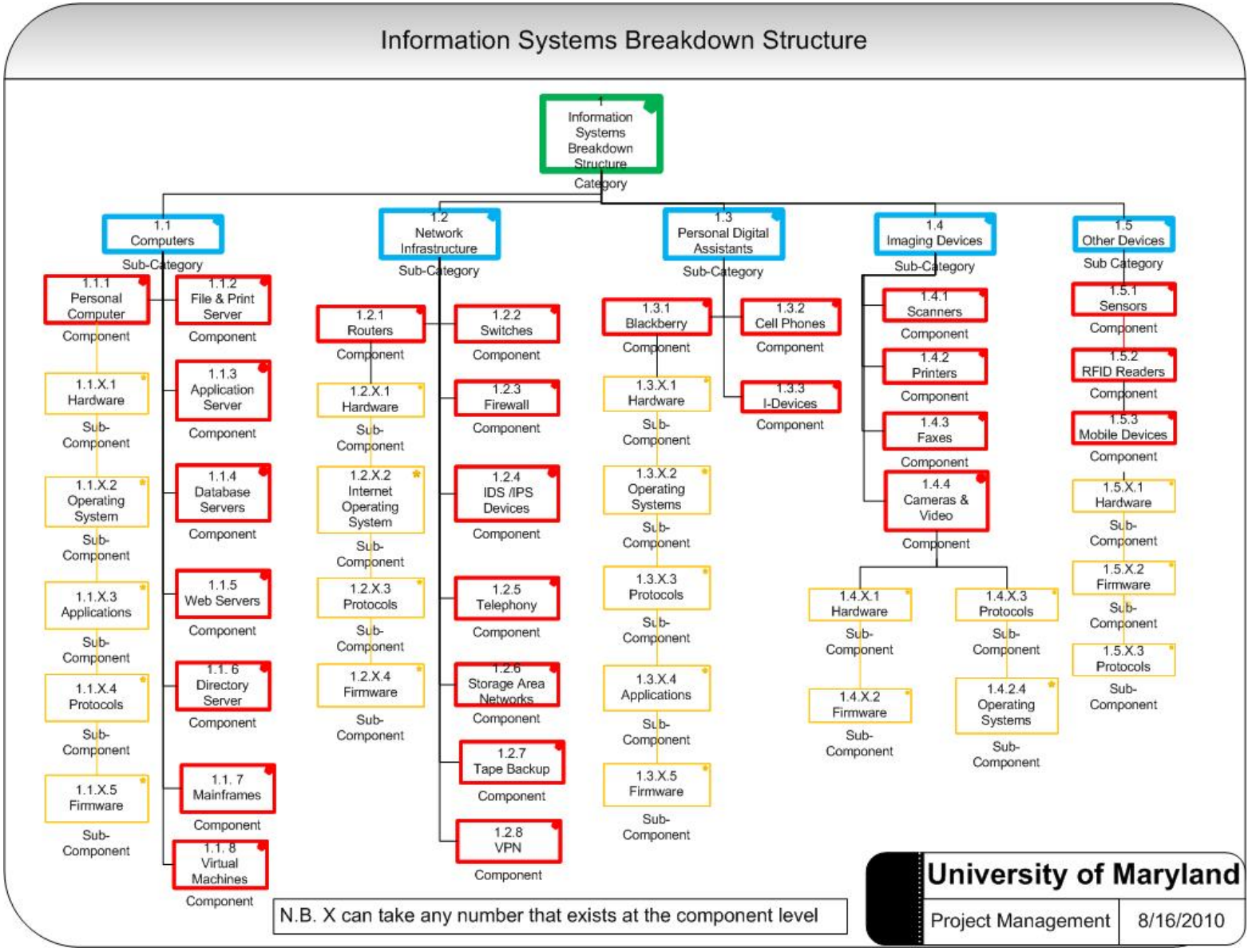
Information Systems Breakdown Structure
Information Systems Breakdown Structure Category
1.1 Computers
Sub-Category
1.1.1 Personal Computer
Component
1.1.X.1 Hardware
Sub-Component
1.1.X.2 Operating System
Sub-Component
1.1.X.3 Applications
Sub-Component
1.1.X.4 Protocols
Sub-Component
1.1.X.5 Firmware
Sub-Component
1.1.2 File & Print Server
Component
1.1.3 Application Server
Component
1.1.4 Database Servers
Component
1.1.5 Web Servers
Component
1.1. 6 Directory Server
Component
1.1. 7 Mainframes
Component
1.1. 8 Virtual Machines
Component
1.2 Network Infrastructure
Sub-Category
1.2.1 Routers
Component
1.2.X.1 Hardware
Sub-Component
1.2.X.2 Internet Operating System
Sub-Component
1.2.X.3 Protocols
Sub-Component
1.2.X.4 Firmware
Sub-Component
1.2.2 Switches
Component
1.2.3 Firewall
Component
1.2.4 IDS /IPS Devices
Component
1.2.5 Telephony
Component
1.2.6 Storage Area Networks
Component
1.2.7 Tape Backup
Component
1.2.8 VPN
Component
1.3 Personal Digital Assistants
Sub-Category
1.3.1 Blackberry
Component
1.3.X.1 Hardware
Sub-Component
1.3.X.2 Operating Systems
Sub-Component
1.3.X.3 Protocols
Sub-Component
1.3.X.4 Applications
Sub-Component
1.3.X.5 Firmware
Sub-Component
1.3.2 Cell Phones
Component
1.3.3 I-Devices
Component
1.4 Imaging Devices
Sub-Category
1.4.1 Scanners
Component
1.4.2 Printers
Component
1.4.3 Faxes
Component
1.4.4 Cameras & Video
Component
1.4.X.1 Hardware
Sub-Component
1.4.X.2 Firmware
Sub-Component
1.4.X.3 Protocols
Sub-Component
1.4.2.4 Operating Systems
Sub-Component
1.5 Other Devices
Sub Category
1.5.1 Sensors
Component
1.5.2 RFID Readers
Component
1.5.3 Mobile Devices
Component
1.5.X.1 Hardware
Sub-Component
1.5.X.2 Firmware
Sub-Component
1.5.X.3 Protocols
Sub-Component
N.B. X can take any number that exists at the component level
University of Maryland
Project Management
8/16/2010

Figure 1.0 Information System Breakdown Structure

For each of the statements below, select whether you strongly disagree, disagree, agree or strongly agree with the statements.

		Strongly disagree	**Disagree**	**Agree**	**Strongly agree**
18.	The sub-categories (computers, network infrastructure, personal digital assistants, imaging device and other devices) identified in Figure 1.0 are sufficient to categorize all information systems.	☐	☐	☐	☐
19.	The components identified for the computers sub-category are sufficient to identify information systems for this sub-category.	☐	☐	☐	☐
20.	The components identified for the network infrastructure sub-category are sufficient to identify information systems for this sub-category.	☐	☐	☐	☐
21.	The components identified for the personal digital assistants sub-category are sufficient to identify information systems for this sub-category.	☐	☐	☐	☐
22.	The components identified for the imaging devices sub-category are sufficient to identify information systems for this sub-category.	☐	☐	☐	☐
23.	The components identified for the other devices sub-category are a sufficient catchall for information systems not identified in the computers, network infrastructure, personal digital assistants and imaging devices sub-categories.	☐	☐	☐	☐
24.	The generic sub-components identified for the different components are sufficient to assess risks at the sub-component levels.	☐	☐	☐	☐
25.	The use of an information system breakdown structure improves the ability of assessors to identify organizational information system assets.	☐	☐	☐	☐

Information System Breakdown Structure Feedback

26. Kindly provide additional feedback for items you disagree or strongly disagree with.

Section 2.1 e-Government Relational Technical Control Validation

The National Institute of Science and Technology (NIST) uses a hierarchical tree structure approach to information security in their development on of the different security control families that belong to either the Management, Operational or Technical Control Family. The NIST security assessment approach is not a relational approach and this result in duplicate security controls as is evident by fifteen security controls withdrawn and merged into other controls for the recently published NIST SP 800-53 Rev 3 of August 2009. The duplicates encountered in the use of current NIST methodology are synonymous with the duplicates encountered when saving records in a flat file. Another issue is one of data integrity between the controls.

The goal of this research is to develop an e-Government Relational Technical control to address the issue of duplicates in the security control and to improve the process of performing security assessment by providing a fully integrated approach to assessing the security controls. The relationships develop for the Technical Controls namely; Identification and Authentication (IA) Control, Access (AC) Control, Audit and Accountability (AU) Control and System and Communications Protection (SC) Control shall be validated in this section of this document. Figure 1 depicts the entity relationships diagram for the Technical Control Family and entities that may access the information system. The diagram also identifies some attributes of the different entities. The current attributes for the NIST Technical Control family are base on the NIST 800-53 Rev 3 document. Please note that the section numbers for this data collection effort are base on the relationships labels provided in Figure 2.

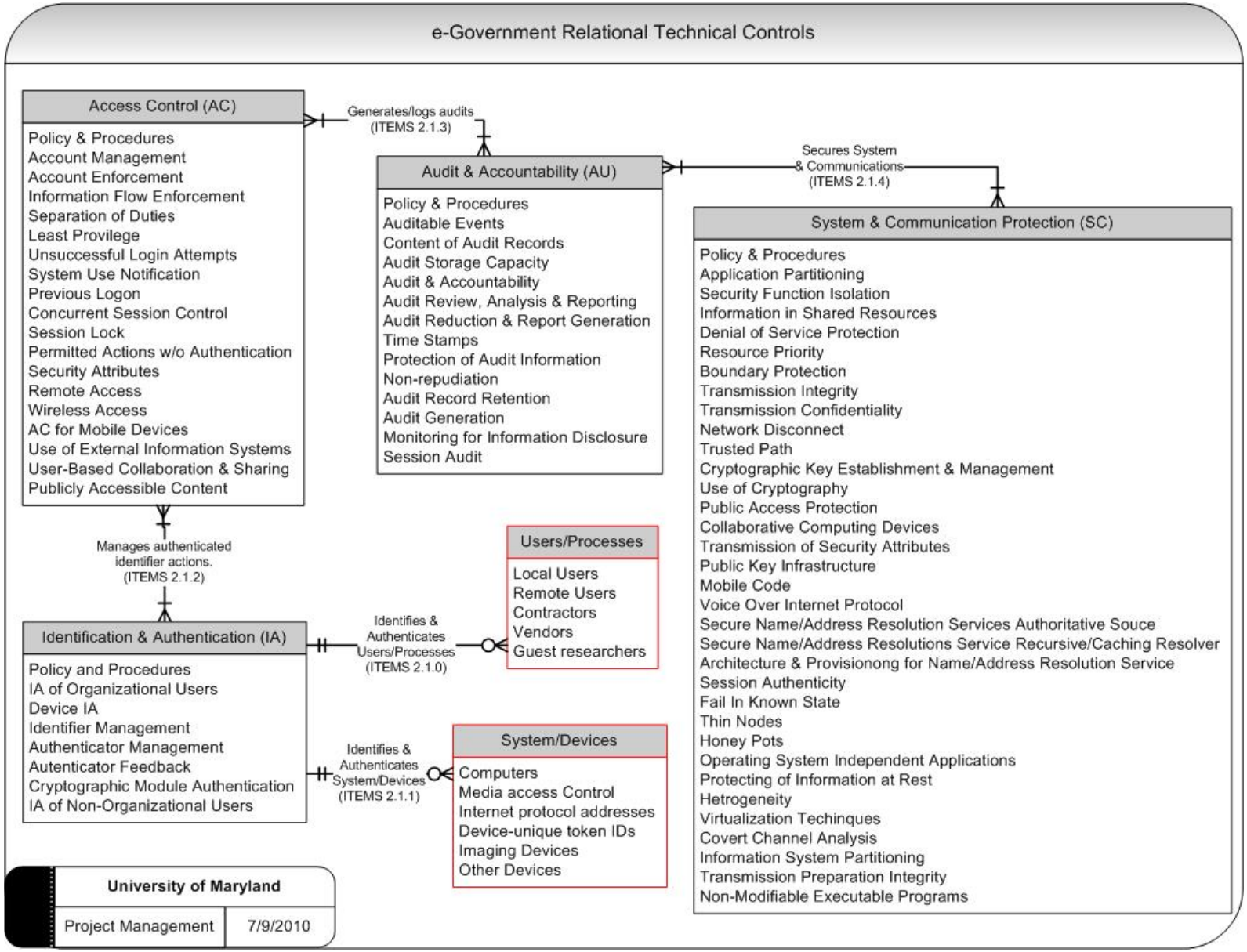
e-Government Relational Technical Controls
Access Control (AC)
Policy & Procedures
Account Management
Account Enforcement
Information Flow Enforcement
Separation of Duties
Least Privilege
Unsuccessful Login Attempts
System Use Notification
Previous Logon
Concurrent Session Control
Session Lock
Permitted Actions w/o Authentication
Security Attributes
Remote Access
Wireless Access
AC for Mobile Devices
Use of External Information Systems
User-Based Collaboration & Sharing
Publicly Accessible Content
Generates/logs audits
(ITEMS 2.1.3)
Audit & Accountability (AU)
Policy & Procedures
Auditable Events
Content of Audit Records
Audit Storage Capacity
Audit & Accountability
Audit Review, Analysis & Reporting
Audit Reduction & Report Generation
Time Stamps
Protection of Audit Information
Non-repudiation
Audit Record Retention
Audit Generation
Monitoring for Information Disclosure
Session Audit
Secures System
& Communications
(ITEMS 2.1.4)
System & Communication Protection (SC)
Policy & Procedures
Application Partitioning
Security Function Isolation
Information in Shared Resources
Denial of Service Protection
Resource Priority
Boundary Protection
Transmission Integrity
Transmission Confidentiality
Network Disconnect
Trusted Path
Cryptographic Key Establishment & Management
Use of Cryptography
Public Access Protection
Collaborative Computing Devices
Transmission of Security Attributes
Public Key Infrastructure
Mobile Code
Voice Over Internet Protocol
Secure Name/Address Resolution Services Authoritative Souce
Secure Name/Address Resolutions Service Recursive/Caching Resolver
Architecture & Provisionong for Name/Address Resolution Service
Session Authenticity
Fail In Known State
Thin Nodes
Honey Pots
Operating System Independent Applications
Protecting of Information at Rest
Hetrogeneity
Virtualization Techinques
Covert Channel Analysis
Information System Partitioning
Transmission Preparation Integrity
Non-Modifiable Executable Programs
Manages authenticated
identifier actions.
(ITEMS 2.1.2)
Identification & Authentication (IA)
Policy and Procedures
IA of Organizational Users
Device IA
Identifier Management
Authenticator Management
Autenticator Feedback
Cryptographic Module Authentication
IA of Non-Organizational Users
Identifies &
Authenticates
Users/Processes
(ITEMS 2.1.0)
Users/Processes
Local Users
Remote Users
Contractors
Vendors
Guest researchers
Identifies &
Authenticates
System/Devices
(ITEMS 2.1.1)
System/Devices
Computers
Media access Control
Internet protocol addresses
Device-unique token IDs
Imaging Devices
Other Devices
University of Maryland
Project Management
7/9/2010

Figure 2. e-Government Relational Technical Controls

ITEMS 2.1.0: Users/Processes & IA Relationship

These items validate the relationships between the IA entity and the Users/Processes entity. For each of the statements below, select whether you strongly disagree, disagree, agree or strongly agree with the statements. The term 'user' used below include processes acting as users but excludes system maintainers.

		Strongly disagree	Disagree	Agree	Strongly agree
27.	Each Users/Processes should have a unique identifier for authentication to an information system.	☐	☐	☐	☐
28.	Users/Processes should be restricted to a single user/process id.	☐	☐	☐	☐
29.	An IA entity should be capable of identification and authentication of multiple users/processes.	☐	☐	☐	☐
30.	An IA entity can exist that does not identify and authenticate users/process. (They may identify and authenticate only systems/devices)	☐	☐	☐	☐

Users/Processes & IA Relationship Feedback

31. Kindly provide additional feedback for items you disagree or strongly disagree with.

ITEMS 2.1.1: System/Devices & IA Relationship

These items validate the relationships between the IA entity and the System/Devices entity. For each of the questions below, please select whether you strongly disagree, disagree, agree or strongly agree with the statements.

		Strongly disagree	Disagree	Agree	Strongly agree
32.	A System/Device should have a unique identifier for authentication to an information system.	☐	☐	☐	☐
33.	A System/Device should be restricted to a single system/device id.	☐	☐	☐	☐
34.	An IA entity should be capable of identification and authentication of multiple systems/devices.	☐	☐	☐	☐
35.	An IA entity can exist that does not identify and authenticate systems/devices (They may identify and authenticate only Users/Processes)	☐	☐	☐	☐

System/Devices & IA Relationship Feedback

36. Kindly provide additional feedback for items you disagree or strongly disagree with.

ITEMS 2.1.2: IA & AC Relationship

These items validate the relationships between the IA and AC entities. For each of the questions below, please select whether you strongly disagree, disagree, agree or strongly agree with the statements.

		Strongly disagree	Disagree	Agree	Strongly Agree
37.	Authenticated identifiers must be granted access to an information system.	☐	☐	☐	☐
38.	Authenticated identifiers may be granted access to multiple information systems.	☐	☐	☐	☐
39.	The access control entity should control the access of at least one authenticated identifier.	☐	☐	☐	☐
40.	The access control entity should be capable of managing the access of multiple authenticated identifiers.	☐	☐	☐	☐

IA & AC Relationship Feedback

41. Kindly provide additional feedback for items you disagree or strongly disagree with.

ITEMS 2.1.3: AC & AU Relationship

These items validate the relationships between the AU and AC entities. For each of the questions below, please select whether you strongly disagree, disagree, agree or strongly agree with the statements.

		Strongly disagree	Disagree	Agree	Strongly Agree
42.	The access control entity must create an audit event record.	☐	☐	☐	☐
43.	The access control entity may create multiple audit events.	☐	☐	☐	☐
44.	The audit and accountability entity must audit an access control entity.	☐	☐	☐	☐
45.	The audit and accountability entity may audit multiple access control entities.	☐	☐	☐	☐

AU & AC Relationship Feedback

46. Kindly provide additional feedback for items you disagree or strongly disagree with.

ITEMS 2.1.4: AU & SC Relationship

These items validate the relationships between the AU and SC entities. For each of the questions below, please select whether you strongly disagree, disagree, agree or strongly agree with the statements.

		Strongly disagree	Disagree	Agree	Strongly Agree
47.	The audit and accountability entity should feed to a system and communication protection entity.	☐	☐	☐	☐
48.	The audit and accountability entity may feed to multiple systems and communication protection entities.	☐	☐	☐	☐
49.	The system and communication protection entity must monitor an audit entity.	☐	☐	☐	☐
50.	The system and communication protection entity may monitor multiple audit entities.	☐	☐	☐	☐

AU & SC Relationship Feedback

51. Kindly provide additional feedback for items you disagree or strongly disagree with.

End of Section 2

Section 3

Section 3.0 Risk Mitigation and Management Strategies

This section shall ask questions to determine the best practices for risk mitigation and management strategies of the Identification and Authentication Family of the NIST Technical Controls for Information Systems. This section aims to identify what security industry practitioners perceive as the most effective risk mitigation and management strategies for the Identification and Authentication Control Family.

ITEMS 3.1.0: Identification & Authentication Risk Management Strategies

To determine the best practices for risk mitigation and management strategies of the Identification and Authentication Control Family for Information Systems. For each of the comment below, please select whether you strongly disagree, disagree, agree or strongly agree with the statements.

		Strongly disagree	Disagree	Agree	Strongly Agree

52.	IA-2: Authenticated user/process IDs should be granted access to the information system.	☐	☐	☐	☐
53.	IA-2: The identification and authentication control family should be use to manage identifier generator for an information system.	☐	☐	☐	☐
54.	IA-2: The identifier management and the access control entities should be integrated for managing access to applications (residing on the information system) and the information system.	☐	☐	☐	☐
55.	IA-2: The use of multi-factor authentication increases the security posture of information systems.	☐	☐	☐	☐
56.	IA-2: Identifier generators should be capable of multi-factor authentication.	☐	☐	☐	☐
57.	IA-2: Having one of the factors of multi-factor authentication provided by a device separate from the information system being access, improves the security posture of the information system.	☐	☐	☐	☐
58.	IA-2: The use of time synchronous or challenge-response one-time authenticators improves the security posture of information systems.	☐	☐	☐	☐

IA-2 Feedback

59. Kindly provide additional feedback for items you disagree or strongly disagree with.

For each of the comment below, please select whether you strongly disagree, disagree, agree or strongly agree with the statements.

		Strongly disagree	Disagree	Agree	Strongly Agree
60.	IA-3: System/device ids should be centrally managed by an information system.	☐	☐	☐	☐
61.	IA-3: The use of MAC addresses for the identification and authentication of devices/systems improves the security posture of an information system.	☐	☐	☐	☐
62.	IA-3: The use of IP addresses for identification and authentication of devices/systems improves the security posture of an information system.	☐	☐	☐	☐
63.	IA-3: The use of bidirectional authentication between devices improves the security posture of an information system.	☐	☐	☐	☐

IA-3 Feedback

64. Kindly provide additional feedback for items you disagree or strongly disagree with.

For each of the comment below, please select whether you strongly disagree, disagree, agree or strongly agree with the statements.

		Strongly disagree	Disagree	Agree	Strongly Agree
65.	IA-4: Users, processes, systems and devices must be uniquely identified to an information system.	☐	☐	☐	☐
66.	IA-4: Preventing the reuse of user, process, system or device identifiers increases the security posture of an information system.	☐	☐	☐	☐
67.	IA-4: Disabling user identifier after an organization-defined period of inactivity improves the security posture of an information system.	☐	☐	☐	☐
68.	IA-4: The use of user identifiers that do not match the email address of users improves the security posture of an information system.	☐	☐	☐	☐

IA-4 Feedback

69. Kindly provide additional feedback for items you disagree or strongly disagree with.

For each of the comments below, please select whether you strongly disagree, disagree, agree or strongly agree with the statements.

		Strongly disagree	Disagree	Agree	Strongly Agree
70.	IA-5: Limiting the reuse of authenticators for users/processes improves the security posture of information systems	☐	☐	☐	☐
71.	IA-5: Limiting the reuse of authenticators for systems/devices improves the security posture of information systems	☐	☐	☐	☐
72.	IA-5: Establishing the minimum period before requiring a password change improves the security posture of information systems.	☐	☐	☐	☐
73.	IA-5: Establishing the maximum period before requiring a password change improves the security posture of information systems.	☐	☐	☐	☐
74.	IA-5: The use of automated tools to determine the strength of authenticators to resist attacks improves the security posture of information system.	☐	☐	☐	☐
75.	IA-5: The use of different unique authenticators (or passwords) for different information systems improves the security posture of the organization.	☐	☐	☐	☐
76.	IA-5: Employing the use of single sign-on improves the security posture of information systems.	☐	☐	☐	☐
77.	IA-5: Using one-time passwords improves the security posture of information systems.	☐	☐	☐	☐
78.	IA-5: Restricting the number of accounts individuals have on multiple information systems improves their security posture.	☐	☐	☐	☐

The ranges below are in days. For each of the questions below select the range (in days) that you believe should be assigned for each question.

		<= 30	31 - 60	61 - 90	91 - 120	>=121

79.	IA-4: What should be the period of inactivity before a user account is disabled?	☐	☐	☐	☐	☐
80.	IA-5: How often should authenticators (or passwords) be changed/refreshed?	☐	☐	☐	☐	☐

81. IA-5: How many password histories should an information system remembers and prevents users from reusing?

- ☐ <=3
- ☐ 4 - 6
- ☐ 7 - 9
- ☐ 10 - 12
- ☐ >= 13

82. IA-5: What should be the minimum number of characters required for passwords?

- ☐ <= 7
- ☐ 8 - 10
- ☐ 11 - 13
- ☐ Other:

83. IA-5: Select the options that you believe improves the security of authenticators. (Select all that apply)

- ☐ Requiring passwords to be case sensitive
- ☐ Requiring that the password exceeds a certain number of characters
- ☐ Requiring the use of both upper and lower case letters
- ☐ Requiring the use of numbers
- ☐ Requiring the use of special characters
- ☐ Having a minimum requirement for each of the items listed above

IA-5 Feedback

84. Kindly provide additional feedback for items you disagree or strongly disagree with.

For each of the statements below, select whether you strongly disagree, disagree, agree or strongly agree with the statements.

		Strongly disagree	Disagree	Agree	Strongly agree
85.	IA-6: Obscuring of feedback during authentication improves the security posture of information systems.	☐	☐	☐	☐
86.	IA-7: The use of cryptographic modules during authentication improves the security posture of information systems.	☐	☐	☐	☐
87.	IA-8: The identification and authentication of non-organizational users improves the security posture of the information system.	☐	☐	☐	☐

IA-6, IA-7, IA-8 Feedback

88. Kindly provide additional feedback for items you disagree or strongly disagree with.

End of Section 3

Section 4

Section 4.0 Duration & Fee for Security Assessments

These questions determine shall help to develop a cost model for determining the cost of performing risk assessment for the identification and authentication control family. The identification and authentication control family is comprised of eight controls and a total of thirty-one enhancements. The questions in this section will cover the duration required to perform security assessments for the identification and authentication control family and the fee that information assurance contractors charge for performing security assessments.

SURVEY INSTRUCTIONS: All the ranges below are in hours. For the question below, select the range (in days) that it took you to complete the following tasks, for your last security assessment of the identification and authentication control family.

		<= 1	2 - 3	4 - 5	6 - 7	>=8
89.	To examine and assess the documents related to the identification and authentication control family.	☐	☐	☐	☐	☐
90.	To complete an interview of organizational stakeholders on the requirements for the identification and authentication control family.	☐	☐	☐	☐	☐
91.	To test the control requirements for the identification and authentication control family.	☐	☐	☐	☐	☐
92.	To develop reports for the identification and authentication control family based on security assessment of its controls.	☐	☐	☐	☐	☐

93. For what organization did you perform the last security assessment?

94. What is the fee (in $/hr) information assurance organizations charge customers for performing security assessments? (Please note that this question is not asking for your hourly salary, but rather what an organization may charge customers for your services.

Duration & Fee Feedback

95. For questions 89 to 92, if you selected a duration greater than or equal to 8 days please specify what you believe the duration should be and why. You may also use this space to provide additional feedback for the entire data collection effort.

End of Section 4

End of the Data Collection

Appendix B: Excluded Interview Questions

This section contains interview questions that are excluded from the research because including them would have resulted in over 300 interview questions and it would have been impossible to find respondents to answer the questions. By excluding questions for the Access Control, Audit and System and Communications Protection Control Families we reduced the interview questions by 149. These questions are provided for future research in this section.

Information System Risk Management Validation

These items shall validate the relationships between the entities of the Information System Risk Management Model shown in Figure 2.

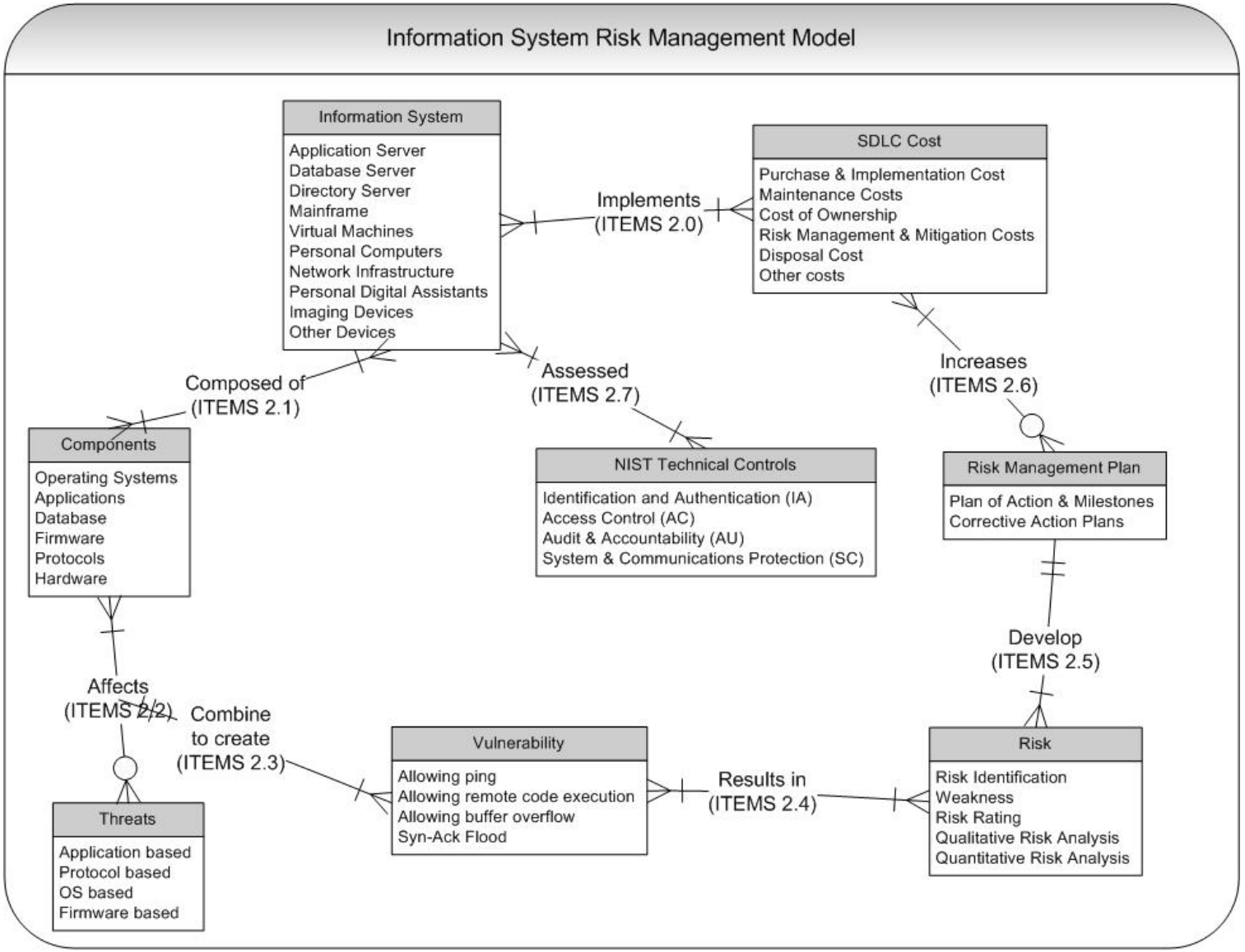

Figure 2. Information System Risk Management Model

ITEMS 2.2.0: SDLC Cost & Information System Relationship

These items validate the relationships between the SDLC Cost and the Information System entities. For each of the questions below, please select whether you strongly disagree, disagree, agree or strongly agree with the statements.

		Strongly disagree	Disagree	Agree	Strongly Agree
50.	The SDLC cost entity should be used to implement an information system.	☐	☐	☐	☐
51.	The SDLC cost entity may be used to implement multiple information systems.	☐	☐	☐	☐
52.	Information Systems cost must belong to an SDLC cost entity	☐	☐	☐	☐
53.	Information System costs may belong to multiple SDLC cost entities	☐	☐	☐	☐

SDLC Cost & Information System Relationship Feedback.

54. Please provide any additional feedback in the space below.

ITEMS 2.2.1: Information System & Components Relationship

These items validates the relationships between the Components and the Information System entities. For each of the questions below, please select whether you strongly disagree, disagree, agree or strongly agree with the statements.

		Strongly disagree	Disagree	Agree	Strongly Agree
55.	An information system entity must contain a component entity.	☐	☐	☐	☐
56.	An information system entity may be composed of multiple component entities.	☐	☐	☐	☐
57.	Component entities may be assembled to form an information system entity.	☐	☐	☐	☐
58.	Component entities may be assembled to form multiple information system entities.	☐	☐	☐	☐

Components & Information System Relationship Feedback.

59. Please provide any additional feedback in the space below.

ITEMS 2.2.2: Threats & Components Relationship

These items validate the relationships between the Components and the Threats entities. For each of the questions below, please select whether you strongly disagree, disagree, agree or strongly agree with the statements.

		Strongly disagree	Disagree	Agree	Strongly Agree
60.	A component entity may be affected by a threat entity.	☐	☐	☐	☐
61.	A component entity may be affected by multiple threat entities.	☐	☐	☐	☐
62.	Threat entities must belong to a component entity.	☐	☐	☐	☐
63.	Threat entities may belong to multiple component entities.	☐	☐	☐	☐

Components & Threat Relationship Feedback.

64. Please provide any additional feedback in the space below.

ITEMS 2.2.3: Component Threats & Vulnerability Relationship

These items validates the relationships between the Component Threats and Vulnerabilities entities. For each of the questions below, please select whether you strongly disagree, disagree, agree or strongly agree with the statements.

		Strongly disagree	Disagree	Agree	Strongly Agree
65.	A component threat results in a vulnerability.	☐	☐	☐	☐
66.	A component threat may result in multiple vulnerability entities	☐	☐	☐	☐
67.	A vulnerability entity must belong on a component threat entity.	☐	☐	☐	☐
68.	A vulnerability entity should map to only one component threat entity.	☐	☐	☐	☐

Component Threats & Vulnerability Relationship Feedback.

70. Please provide any additional feedback in the space below.

ITEMS 2.2.4: Vulnerability & Risk Relationship

These items validate the relationships between the Vulnerability and Risk entities. For each of the questions below, please select whether you strongly disagree, disagree, agree or strongly agree with the statements.

		Strongly disagree	Disagree	Agree	Strongly Agree
70.	A vulnerability entity results in a risk entity.	☐	☐	☐	☐
71.	A vulnerability entity may result in multiple risks entities.	☐	☐	☐	☐
72.	A risk entity is a result of at least one vulnerability entity.	☐	☐	☐	☐
73.	A risk entity may be a result of multiple vulnerability entities.	☐	☐	☐	☐

Vulnerability & Risk Relationship Feedback.

74. Please provide any additional feedback in the space below.

ITEMS 2.2.5: Risk & Risk Management Plans Relationship

These items validate the relationships between the Risk and the Risk Management Plan entities. For each of the questions below, please select whether you strongly disagree, disagree, agree or strongly agree with the statements.

		Strongly disagree	Disagree	Agree	Strongly Agree
75.	A risk entity must track to a risk management plan.	☐	☐	☐	☐
76.	A risk entity must not track to multiple risk management plans.	☐	☐	☐	☐
77.	A risk management plan must contain a risk entity.	☐	☐	☐	☐
78.	A risk management plan may contain multiple risk entities.	☐	☐	☐	☐

Risk & Risk Management Plan Relationship Feedback.

79. Please provide any additional feedback in the space below.

ITEMS 2.2.6: Risk Management Plans & SDLC Cost Relationship

These items validates the relationships between the Risk Management Plan and SDLC cost entities. For each of the questions below, please select whether you strongly disagree, disagree, agree or strongly agree with the statements.

		Strongly disagree	Disagree	Agree	Strongly Agree
80.	A risk management plan entity increases a SDLC Cost entity.	☐	☐	☐	☐
81.	A risk management plan entity may increase multiple SDLC cost entities.	☐	☐	☐	☐
82.	A SDLC Cost may include a risk management plan entity.	☐	☐	☐	☐
83.	A SDLC Cost may include multiple Risk Management Plan entities.	☐	☐	☐	☐

Risk Management Plan & SDLC Cost Relationship Feedback.

84. Please provide any additional feedback in the space below.

ITEMS 2.2.7: Information System & NIST Technical Controls Relationship

These items validates the relationships between the Information System and the NIST Technical Control entities. For each of the comment below, please select whether you strongly disagree, disagree, agree or strongly agree with the statements.

		Strongly disagree	Disagree	Agree	Strongly Agree
85.	The information system entity may be assess with a NIST Technical Control Entity	☐	☐	☐	☐
86.	The information system may be assessed with multiple NIST Technical Control entitles	☐	☐	☐	☐
87.	NIST Technical Control Entities must apply to an information system	☐	☐	☐	☐
88.	NIST Technical Control entities may apply to multiple information systems	☐	☐	☐	☐

Information System & NIST Technical Controls Relationship Feedback.

89. Please provide any additional feedback in the space below.

ITEMS 3.1.1: Access Control Risk Management Strategies

To determine the best practices for risk mitigation and management strategies of the Access Control Family. For each of the statements below, select whether you strongly disagree, disagree, agree or strongly agree with the statements.

		Strongly disagree	Disagree	Agree	Strongly agree
133.	AC-2: The efficient and timely management of information system accounts improves the security posture of the information system.	☐	☐	☐	☐
134.	AC-2: IA-2 (The information system uniquely identifies and authenticates organizational users) should be merged with AC-2 (The organization manages information system accounts).	☐	☐	☐	☐
135.	AC-2: Restricting access to the information system to specific times of the day improves the security posture of the information system.	☐	☐	☐	☐
136.	AC-2: Auditing for atypical usage of information system accounts improves the security posture of information systems.	☐	☐	☐	☐
137.	AC-2: The information system dynamically manages user accounts improves its security posture.	☐	☐	☐	☐
138.	AC-2: The use of robe-based access control as opposed to dynamic account management improves the security posture of the information system.	☐	☐	☐	☐

139. AC-2: What do you believe should be the duration of inactivity before a user is logged out of the information system?

☐ <= 10 minutes

☐ 11 - 20 minutes

☐ 21 - 30 minutes

☐ 31 - 40 minutes

☐ 41 - 50 minutes

☐ 51 - 60 minutes

☐ > 61 minutes

AC-2 Feedback.

140. Please provide any additional feedback in the space below.

For each of the statements below, select whether you strongly disagree, disagree, agree or strongly agree with the statements.

		Strongly disagree	Disagree	Agree	Strongly agree
141.	AC-3: The use of mandatory access control improves the security posture of information systems.	☐	☐	☐	☐
142.	AC-3: The use of role based access control improves the security posture of information systems.	☐	☐	☐	☐
143.	AC-3: The use of discretionary access control improves the security posture of information systems.	☐	☐	☐	☐

AC-3 Feedback.

144. Please provide any additional feedback in the space below.

For each of the statements below, select whether you strongly disagree, disagree, agree or strongly agree with the statements.

		Strongly disagree	Disagree	Agree	Strongly agree
145.	AC-4: Keeping export controlled information from being transmitted in clear to the Internet improves the security posture of information system.	☐	☐	☐	☐
146.	AC-4: The use of a web proxy improves the security posture of the information system.	☐	☐	☐	☐
147.	AC-4: The use of one-way information flow improves the security posture of information systems.	☐	☐	☐	☐
148.	AC-4: The use of information flow control entities improves the security posture of information systems.	☐	☐	☐	☐

AC-4 Feedback.

149. Please provide any additional feedback in the space below.

For each of the statements below, select whether you strongly disagree, disagree, agree or strongly agree with the statements.

		Strongly disagree	Disagree	Agree	Strongly agree
150.	AC-5: The use of separation of duties improves the security posture of the information system.	☐	☐	☐	☐
151.	AC-5: The use of separation of duties improves the security posture of the organization.	☐	☐	☐	☐
152.	AC-6: The use of least privilege principle improve the security posture of information systems.	☐	☐	☐	☐
153.	AC-6: The use of least privilege principle improves the security posture of the organization.	☐	☐	☐	☐
154.	AC-5: (Separation of duties) should be merged with AC-3 (Access Enforcement)	☐	☐	☐	☐
155.	AC-6: (Least privilege) should be merged with AC-3 (Access Enforcement)	☐	☐	☐	☐
156.	AC-6: The use of multiple accounts by the same user for security and non-security functions improves the security posture of the information system.	☐	☐	☐	☐
157.	AC-6: Employing virtualization techniques to control user access improves the security posture of the information system.	☐	☐	☐	☐

AC-5, AC-6 Feedback.

158. Please provide any additional feedback in the space below.

For each of the statements below, select whether you strongly disagree, disagree, agree or strongly agree with the statements.

		Strongly disagree	Disagree	Agree	Strongly agree

		Strongly disagree	Disagree	Agree	Strongly agree
159.	AC-7: The use of account lockout (until enabled by an administrator) for user login attempts that reach the unsuccessful login threshold improves the security posture of information systems.	☐	☐	☐	☐
160.	AC-7: The unsuccessful login attempt delay period should be different for all systems within an organization.	☐	☐	☐	☐
161.	AC-7: The ability to purge the information on mobile devices when the number of unsuccessful login attempts is reached improves the security posture of the information system.	☐	☐	☐	☐
162.	AC-8: System use notification prior to login improves the security posture of the information system.	☐	☐	☐	☐
163.	AC-9: Previous logon (access) notification improves the security posture of the information system.	☐	☐	☐	☐
164.	AC-10: The use of concurrent session control improves the security posture of the information system.	☐	☐	☐	☐
165.	AC-11: The use of session lock improves the security posture of the information system.	☐	☐	☐	☐

Select a range (in minutes) for each of the questions below. AC-7: Unsuccessful Login Attempts

		<= 15 mins	16 - 30 mins	31 - 45 mins	46 - 60 mins	>= 61 mins
166.	What should be the duration (in minutes) for account lockout due to unsuccessful login attempts?	☐	☐	☐	☐	☐
167.	What should be the duration for the delay next login prompt?	☐	☐	☐	☐	☐

168. Unsuccessful login attempts should be restricted to how many attempts? AC-7: Unsuccessful Login Attempts

- ☐ 1 - 3
- ☐ 4 - 6
- ☐ 7 - 9
- ☐ 10 - 12
- ☐ Other: ____

AC-7, AC-8, AC-9, AC-10, AC-11 Feedback.

169. Please provide any additional feedback in the space below.

For each of the statements below, select whether you strongly disagree, disagree, agree or strongly agree with the statements.

		Strongly disagree	Disagree	Agree	Strongly agree
170.	AC-14: No actions should be allowed on the information system without identification and authentication.	☐	☐	☐	☐
171.	AC-14: Access to public information on the web interface of information system may be granted without identification and authentication.	☐	☐	☐	☐
172.	AC-16: The use of security attributes for controlling access to subjects and objects improves the security posture of the information system.	☐	☐	☐	☐
173.	AC-16 (Security Attributes) should be merged with AC-3 (Access Enforcement)	☐	☐	☐	☐
174.	AC-17: Use of VPN for remote access improves the security posture of	☐	☐	☐	☐

		Strongly disagree	Disagree	Agree	Strongly agree
	the information system.				
175.	AC-17 (Remote Access) should be merged with AC-3 (Access Enforcement)	☐	☐	☐	☐
176.	AC-17: The use of cryptography to ensure the confidentiality and integrity of remote access, improves the security posture of the information system.	☐	☐	☐	☐
177.	AC-17: Centralized management of remote access improves the security posture of the information system.	☐	☐	☐	☐

C-14, AC-16, AC-17 Feedback.

178. Please provide any additional feedback in the space below.

For each of the statements below, select whether you strongly disagree, disagree, agree or strongly agree with the statements.
Mobile devices include portable storage media (e.g. USB memory sticks, external hard disk drives) and portable computing and communications devices with information storage capability (e.g. notebook/laptop computers, personal digital assistants, cellular telephones, digital cameras and audio recording devices).

		Strongly disagree	Disagree	Agree	Strongly agree
179.	AC-18: Prohibiting the use of wireless access improves the security posture of the information system.	☐	☐	☐	☐
180.	AC-18: The use of TEMPEST to control wireless emanations improves the security posture of the information system.	☐	☐	☐	☐
181.	AC-18: The use of point-to-point networking with wireless configurations improves the security posture of the information system.	☐	☐	☐	☐

		Strongly disagree	Disagree	Agree	Strongly agree
182.	AC-19: Restricting the use of organizational mobile devices improves the security posture of the information system.	☐	☐	☐	☐
183.	AC-19: Prohibiting the use of mobile devices improves the security posture of the information system.	☐	☐	☐	☐
184.	AC-19: Restricting the use of personal (as opposed to organizational) mobile devices improves the security posture of the information system.	☐	☐	☐	☐
185.	AC-19: Prohibiting the use of personal (as opposed to organizational) mobile devices improves the security posture of the information system.	☐	☐	☐	☐
186.	AC-19: Disabling information system functionality that allows automatic execution of code on mobile devices without user direction (e.g. AutoRun & AutoPlay) improves the security posture of information systems.	☐	☐	☐	☐
187.	AC-19: Prohibiting the use of unclassified mobile devices in facilities containing information systems processing, storing or transmitting classified information improves the securing posture of the information system.	☐	☐	☐	☐
188.	AC-20: Restricting the use of external information system improves the security posture of the information system.	☐	☐	☐	☐
189.	AC-21: Restricting the use of user-based collaboration and information system improves the security posture of the information system.	☐	☐	☐	☐
190.	AC-22: The management of who can post publicly accessible content improves the security posture of the information system.	☐	☐	☐	☐

AC-18, AC-19, AC-20, AC-21, AC-22 Feedback.

191. Please provide any additional feedback in the space below.

ITEMS 3.1.2: Audit Risk Management Strategies

To determine the best practices for risk mitigation and management strategies of the Audit Control Family for Information Systems. For each of the statements below, select whether you strongly disagree, disagree, agree or strongly agree with the statements.

		Strongly disagree	**Disagree**	**Agree**	**Strongly Agree**
192.	AU-2: The identification of auditable events for the information system improves its security posture.	☐	☐	☐	☐
193.	AU-2: The auditing of privileged functions for the information system improves its security posture.	☐	☐	☐	☐
194.	AU-3: The central management of audit records for an information system improves its security posture.	☐	☐	☐	☐
195.	AU-4: The allocating and monitoring of audit storage capacity for an information system improves its security posture.	☐	☐	☐	☐
196.	AU-5: The AU-5 (Response to audit processing failures) should belong to the System and Communication Protection Family of Controls.	☐	☐	☐	☐
197.	AU-5: The ability of an information system to shut down due to audit processing failures improves its security posture.	☐	☐	☐	☐
198.	AU-5: The ability of an information system to overwrite oldest audit records due to audit processing failures improves its security posture.	☐	☐	☐	☐

		Strongly disagree	Disagree	Agree	Strongly Agree
199.	AU-5: The ability of an information system to stop generating audit records due to audit processing failures improves its security posture.	☐	☐	☐	☐

AU-2, AU-3, AU-4, AU-5 Feedback.

200. Please provide any additional feedback in the space below.

201. AU-6: Select the check box below that indicates how often you believe information audit records should be reviewed to provide the most value and security to the information system?

- ☐ Hourly
- ☐ Daily
- ☐ Weekly
- ☐ Monthly
- ☐ Annually

AU-6 Feedback.

202. Please provide any additional feedback in the space below.

For each of the statements below, select whether you strongly disagree, disagree, agree or strongly agree with the statements.

		Strongly disagree	**Disagree**	**Agree**	**Strongly Agree**
203.	AU-6: The ability to integrate audit records with vulnerability scanning information, performance data and network monitoring improve the ability to identity inappropriate/suspicious/malevolent activity for the information system.	☐	☐	☐	☐
204.	AU-6: The ability to integrate audit records with information obtained from monitoring physical access improves the ability to identify suspicious, inappropriate, unusual or malevolent activity.	☐	☐	☐	☐
205.	AU-6: The use of automated mechanisms to alert security personnel should belong to the System and Communication Protection Control Family	☐	☐	☐	☐
206.	AU-6: The use of automate mechanisms to alert security personnel on activities being audited improves the security posture of the information system.	☐	☐	☐	☐
207.	AU-7: The ability of the information system to automatically process audit records for selectable events improves its security posture.	☐	☐	☐	☐

		Strongly disagree	Disagree	Agree	Strongly Agree
208.	AU-8: The proper synchronization of time for the information system improves the ability to establish the sequence of audit events based on their timestamps and improves its security posture.	☐	☐	☐	☐
209.	AU-9: The AC-9 (Protecting of Audit Information) control should fall within the access control family.	☐	☐	☐	☐
210.	AU-9: The ability of the information system to effectively protect audit information improves its security posture.	☐	☐	☐	☐
211.	AU-9: The use of write-once media (like CD-ROMs) to store information system audit records improves the security posture of the information system.	☐	☐	☐	☐
212.	AU-9: The ability of the information system to store audit records onto a different system or media than the one being audited improves its security posture.	☐	☐	☐	☐
213.	AU-9: The use of cryptographic mechanisms to protect the integrity of audit information and audit tools improves the security posture of information system.	☐	☐	☐	☐
214.	AU-9: The ability to limit the number of privilege users who have access to audit functions of an information system improves its security posture.	☐	☐	☐	☐

AU-6, AU-7, AU-8, AU-9 Feedback.

215. Please provide any additional feedback in the space below.

For each of the statements below, select whether you strongly disagree, disagree, agree or strongly agree with the statements.

		Strongly disagree	Disagree	Agree	Strongly Agree
216.	AU-10: The use of private keys digital signatures for non-repudiation on information system improves the security posture of the information system.	☐	☐	☐	☐
217.	AU-10: The binding of information at the time of generation to its producer's identity ensures that the information generated is properly classified for the information system.	☐	☐	☐	☐
218.	AU-11: The definition of the period for retention of audit records should be based on the security categorization of the system, Federal and State statutes and the organizational policy for the different records.	☐	☐	☐	☐
219.	AU-12: The ability for designated organizational personnel to select auditable events for specific components of an information system improves its security posture.	☐	☐	☐	☐
220.	AU-13: The monitoring of open source information for evidence of unauthorized exfiltration or disclosure of organizational information improves the security of the information system.	☐	☐	☐	☐
221.	AU-14: The ability of an information system to audit all content related to user session improves its security posture.	☐	☐	☐	☐

		Strongly disagree	Disagree	Agree	Strongly Agree
222.	AU-14: The ability of an information system to remotely view/hear all content related to an established session in real time improves its security posture.	☐	☐	☐	☐

AU-10, AU-11, AU-12, AU-13, AU-14 Feedback.

223. Please provide any additional feedback in the space below.

ITEMS 3.1.3: System and Communications Protection Risk Management Strategies

To determine the best practices for risk mitigation and management strategies of the System and Communications Protection Control Family for Information Systems. For each of the statements below, select whether you strongly disagree, disagree, agree or strongly agree with the statements.

		Strongly disagree	Disagree	Agree	Strongly Agree
224.	SC-2: The ability of the information system to separate user functionality and services from information system management functionality improves the security posture of the information system.	☐	☐	☐	☐
225.	SC-3: The ability of the information system to isolate security functions from non-security functions improves its security posture.	☐	☐	☐	☐
226.	SC-3: The use of hardware separation mechanisms to facilitate security function isolation improves the security posture of the information system.	☐	☐	☐	☐
227.	SC-3: The implementation of security functions as independent modules that inhibit interactions between modules improves the security posture of the information system.	☐	☐	☐	☐
228.	SC-4: The ability of an information system to partition resources that are used to interface with systems operating at different security levels improves its security posture.	☐	☐	☐	☐
229.	SC-5: The ability of an information system to prevent denial of	☐	☐	☐	☐

		Strongly disagree	Disagree	Agree	Strongly Agree
	service attacks improves its security posture.				
230.	SC-5: The ability of an information system to prevent users from launching a denial of service attack against other systems or networks improves the security posture of the organization.	☐	☐	☐	☐
231.	SC-6: The ability of an information system to limit the use of resources by priority improves its security posture.	☐	☐	☐	☐

SC-2, SC-3, SC-4, SC-5, SC-6 Feedback.

232. Please provide any additional feedback in the space below.

For each of the statements below, select whether you strongly disagree, disagree, agree or strongly agree with the statements.

		Strongly disagree	Disagree	Agree	Strongly agree
233.	SC-7: The ability of the information system to monitor and control communication at external boundaries improves its security posture.	☐	☐	☐	☐
234.	SC-7: The ability of the information system to monitor and control communication at key internal boundaries improves its security posture.	☐	☐	☐	☐
235.	SC-7: The allocation of publicly accessible information system	☐	☐	☐	☐

		Strongly disagree	Disagree	Agree	Strongly agree
	components to separate sub networks having separate physical NIC improves the security posture of an information system.				
236.	SC-7: The ability of an information to deny all traffic by default and allow network traffic by exception improves it security posture.	☐	☐	☐	☐
237.	SC-7: The user of deep packet inspection firewalls and XLM gateways (that can screen data at the application layer for information system) improves the security posture of information system.	☐	☐	☐	☐
238.	SC-7: The use of host based boundary protection for servers improves their security posture	☐	☐	☐	☐
239.	SC-7: The use of host based boundary protection for workstations improves their security posture	☐	☐	☐	☐
240.	SC-7: The use of host based boundary protection for mobile devices improves their security posture	☐	☐	☐	☐
241.	SC-7 The ability of the information system to prevent discovery of its system specific components or devices (example network address is not entered in a domain system) improves its security posture	☐	☐	☐	☐

SC-7 Feedback.

242. Please provide any additional feedback in the space below.

For each of the statements below, select whether you strongly disagree, disagree, agree or strongly agree with the statements.

		Strongly disagree	Disagree	Agree	Strongly agree
243.	SC-8: The ability of the information system to protect the integrity of transmitted information improves its security posture.	☐	☐	☐	☐
244.	SC-8: The ability of the information system to employ cryptographic mechanisms to recognize changes to information during transmission improves its security posture.	☐	☐	☐	☐
245.	SC-9: The ability of the information system to protect the confidentiality of transmitted information improves its security posture.	☐	☐	☐	☐
246.	SC-10: The ability of an information system to terminate a network connection at the end of a session or a period of inactivity improves its security posture.	☐	☐	☐	☐
247.	SC-11:The ability of an information system to establish and maintain a trusted communication path between a user and security functions improves its security posture.	☐	☐	☐	☐
248.	SC-12 The ability of an information system to establish, maintain and manage cryptographic key improves its security posture.	☐	☐	☐	☐

SC-8, SC-9, SC-10, SC-11, SC-12 Feedback.

249. Please provide any additional feedback in the space below.

For each of the statements below, select whether you strongly disagree, disagree, agree or strongly agree with the statements.

		Strongly disagree	Disagree	Agree	Strongly agree
250.	SC-13: The use of cryptography that is consistent with the security classification of the information system improves the security posture of the organization.	☐	☐	☐	☐
251.	SC-14: The ability of the information system to protect the integrity and availability of publicly available information and applications improves its security posture.	☐	☐	☐	☐
252.	SC-15: The ability of an information system to prohibit remote activation of collaborative computer devices improves its security posture.	☐	☐	☐	☐
253.	SC-15: The ability of an information system to provide indication of use to users physically present at the device improves the security posture of the organization.	☐	☐	☐	☐
254.	SC-15: The ability of an information system to provide physical disconnect of a collaborative computing device in a manner that support ease of use improves its security posture.	☐	☐	☐	☐
255.	SC-15: The ability of an information system to block both inbound and outbound traffic between instant messaging clients configured by end users or external service providers improves its security posture.	☐	☐	☐	☐
256.	SC-16: The ability of an information system to associate	☐	☐	☐	☐

		Strongly disagree	Disagree	Agree	Strongly agree
	attributes for information exchanged between systems improves its security posture.				

SC-13, SC-14, SC-15, SC-16 Feedback.

257. Please provide any additional feedback in the space below.

For each of the statements below, select whether you strongly disagree, disagree, agree or strongly agree with the statements.

		Strongly disagree	Disagree	Agree	Strongly agree
258.	SC-17: The use of PKI certificates by the information system improves its security posture.	☐	☐	☐	☐
259.	SC-18: The ability of an information system to detect, inspect and manage mobile code improves its security posture.	☐	☐	☐	☐
260.	SC-19: The ability to authorize, monitor and control the use of VoIP within an information system improves its security posture.	☐	☐	☐	☐
261.	SC-20: The ability of an information system to provide data origin and integrity artifacts along with authoritative data the system returns (in response to a name/address resolutions query) improves its security posture.	☐	☐	☐	☐
262.	SC-21: The ability of an information system to perform data origin authentication and data integrity verification (on the name/address resolution responses the system received from authoritative sources when requested by clients) improves it security posture.	☐	☐	☐	☐
263.	SC-22: The use of a primary and secondary, internal and external authoritative domain name system (DNS) to ensure fault-tolerance improves the security posture of the information system.	☐	☐	☐	☐

SC-17, SC-18, SC-19, SC-20, SC-21, SC-22 Feedback.

264. Please provide any additional feedback in the space below.

For each of the statements below, select whether you strongly disagree, disagree, agree or strongly agree with the statements.

		Strongly disagree	Disagree	Agree	Strongly agree
265.	SC-23: The ability of an information system to protect the authenticity of communications sessions improves it security posture.	☐	☐	☐	☐
266.	SC-23: The ability of an information system to generate session identifiers that are unique for each session and system specific improves its security posture.	☐	☐	☐	☐
267.	SC-24: The ability of an information system to fail in a known state improves its security posture.	☐	☐	☐	☐
268.	SC-25: The use of thin nodes that provide minimal functionality and information storage for an information system improves its security posture.	☐	☐	☐	☐
269.	SC-26: The use of honey pots in the infrastructure of the information system improves its security posture.	☐	☐	☐	☐
270.	SC-27: The use of operating system independent applications (that can run on multiple operating systems) promotes the portability and availability of the information system.	☐	☐	☐	☐

SC-23, SC-24, SC-25, SC-26, SC-27 Feedback.

271. Please provide any additional feedback in the space below.

For each of the statements below, select whether you strongly disagree, disagree, agree or strongly agree with the statements.

		Strongly disagree	Disagree	Agree	Strongly agree
272.	SC-28: The ability of an information system to protect information at rest improves its security posture.	☐	☐	☐	☐
273.	SC-29: The use of diverse information technologies for the implementation of an information system improves the security posture of the information system.	☐	☐	☐	☐
274.	SC-30: The use of virtualization techniques to disguise information systems and its components improves its security posture.	☐	☐	☐	☐
275.	SC-31: The requirement for information system developers to perform covert channel analysis to identify aspects of system communications that are potential avenues for covert storage and timing channels improves the security posture of an information system.	☐	☐	☐	☐

SC-28, SC-29, SC-30, SC-31 Feedback.

276. Please provide any additional feedback in the space below.

For each of the statements below, select whether you strongly disagree, disagree, agree or strongly agree with the statements.

		Strongly disagree	Disagree	Agree	Strongly agree
277.	SC-32: The partitioning of an information system into components residing in separate physical domains/environments improves its security posture.	☐	☐	☐	☐
278.	SC-33: The ability an information system to protect the integrity of information during the process of data aggregation, packaging and transformation in preparation for transmission improves its security posture.	☐	☐	☐	☐
279.	SC-34: The ability of an information system to load and execute its operating environment from hardware enforced or read only media improves its security posture.	☐	☐	☐	☐
280.	SC-34: The ability of an information system to load and execute its applications from hardware enforce or read only media improves its security posture.	☐	☐	☐	☐

SC-32, SC-33, SC-34 Feedback.

281. Please provide any additional feedback in the space below.

Appendix C: Software Results & Analysis Tables

Table C1 Correlation between FISMA and Security Assessment for the Respondents

			FISMAExp.12 12. FISMA Exp.	Sec.Ass.Exp.13 13. Sec. Ass. Exp.
Spearman's rho	FISMAExp.12 12. FISMA Exp.	Correlation Coefficient	1.000	.878**
		Sig. (2-tailed)	.	.000
		N	22	22
	Sec.Ass.Exp.13 13. Sec. Ass. Exp.	Correlation Coefficient	.878**	1.000
		Sig. (2-tailed)	.000	.
		N	22	22

**. Correlation is significant at the 0.01 level (2-tailed).

Table C2 Association between FISMA and Security Assessment Results

			Value	Asymp. Std. Error[a]	Approx. T[b]	Approx. Sig.
Ordinal by Ordinal	Somers' d	Symmetric	.872	.091	6.364	.000
		FISMAExp.12 12. FISMA Exp. Dependent	.872	.091	6.364	.000
		Sec.Ass.Exp.13 13. Sec. Ass. Exp. Dependent	.872	.091	6.364	.000

a. Not assuming the null hypothesis.

			Value	Asymp. Std. Error[a]	Approx. T[b]	Approx. Sig.
Ordinal by Ordinal	Somers' d	Symmetric	.872	.091	6.364	.000
		FISMAExp.12 12. FISMA Exp. Dependent	.872	.091	6.364	.000
		Sec.Ass.Exp.13 13. Sec. Ass. Exp. Dependent	.872	.091	6.364	.000

a. Not assuming the null hypothesis.

b. Using the asymptotic standard error assuming the null hypothesis.

Table C3. Comparison of Dummy Variable for FISMA and Security Assessment Experience

			DummyFISMAExp.12 Recode of FISMAExp to 3 years or less & 4 years or more.	DummySecAssExp.13 Recode of SecAsseExp to 3 years or less & 4 years or more.
Spearman's rho	DummyFISMAExp.12 Recode of FISMAExp to 3 years or less & 4 years or more.	Correlation Coefficient	1.000	.812**
		Sig. (2-tailed)	.	.000
		N	22	22
	DummySecAssExp.13 Recode of SecAsseExp to 3 years or less & 4 years or more.	Correlation Coefficient	.812**	1.000
		Sig. (2-tailed)	.000	.
		N	22	22

**. Correlation is significant at the 0.01 level (2-tailed).

Table C4 Dummy of NetAdmin and NetSec Variables

			DummyNetAdminExp.10 Recode of NetworkAdminExp to 3 years or less & 4 years or more.	DummyNetSecExp.11 Recode of NetSecExp to 3 years or less & 4 years or more.
Spearman's rho	DummyNetAdminExp.10 Recode of NetworkAdminExp to 3 years or less & 4 years or more.	Correlation Coefficient	1.000	.156
		Sig. (2-tailed)	.	.488
		N	22	22
	DummyNetSecExp.11 Recode of NetSecExp to 3 years or less & 4 years or more.	Correlation Coefficient	.156	1.000
		Sig. (2-tailed)	.488	.
		N	22	22

Table C5 Dummy of NetSec and FISMA Variables

			DummyNetSecExp.11 Recode of NetSecExp to 3 years or less & 4 years or more.	DummyFISMAExp.12 Recode of FISMAExp to 3 years or less & 4 years or more.
Spearman's rho	DummyNetSecExp.11 Recode of NetSecExp to 3 years or less & 4 years or more.	Correlation Coefficient	1.000	.478*
		Sig. (2-tailed)	.	.025
		N	22	22
	DummyFISMAExp.12 Recode of FISMAExp to 3 years or less & 4 years or more.	Correlation Coefficient	.478*	1.000
		Sig. (2-tailed)	.025	.
		N	22	22

*. Correlation is significant at the 0.05 level (2-tailed).

Table C6 Bivariate Analysis for FISMA, SecAss, NetAdmin and NetSec Experience

			FISMAExp.12 12. FISMA Exp.	Sec.Ass.Exp.13 13. Sec. Ass. Exp.	Net.Admin.Exp. 10 10. Net. Admin. Exp.	Net.Sec.Exp.11 11. Net. Sec. Exp.
Spearman's rho	FISMAExp.12 12. FISMA Exp.	Correlation Coefficient	1.000	.878**	-.121	.485*
		Sig. (2-tailed)	.	.000	.592	.022
		N	22	22	22	22
	Sec.Ass.Exp.13 13. Sec. Ass. Exp.	Correlation Coefficient	.878**	1.000	-.188	.485*
		Sig. (2-tailed)	.000	.	.403	.022
		N	22	22	22	22
	Net.Admin.Exp.10 10. Net. Admin. Exp.	Correlation Coefficient	-.121	-.188	1.000	-.051
		Sig. (2-tailed)	.592	.403	.	.822
		N	22	22	22	22
	Net.Sec.Exp.11 11. Net. Sec. Exp.	Correlation Coefficient	.485*	.485*	-.051	1.000
		Sig. (2-tailed)	.022	.022	.822	.
		N	22	22	22	22

**. Correlation is significant at the 0.01 level (2-tailed).

*. Correlation is significant at the 0.05 level (2-tailed).

Table C7 Dummy of NetAdmin and FISMA Experience

			DummyNetAdminExp.10 Recode of NetworkAdminExp to 3 years or less & 4 years or more.	DummyFISMAExp.12 Recode of FISMAExp to 3 years or less & 4 years or more.
Spearman's rho	DummyNetAdminExp.10 Recode of NetworkAdminExp to 3 years or less & 4 years or more.	Correlation Coefficient	1.000	.087
		Sig. (2-tailed)	.	.700
		N	22	22
	DummyFISMAExp.12 Recode of FISMAExp to 3 years or less & 4 years or more.	Correlation Coefficient	.087	1.000
		Sig. (2-tailed)	.700	.
		N	22	22

Table C8 Dummy of NetSec and SecAss

			DummyNetSecExp.11 Recode of NetSecExp to 3 years or less & 4 years or more.	DummySecAssExp.13 Recode of SecAsseExp to 3 years or less & 4 years or more.
Spearman's rho	DummyNetSecExp.11 Recode of NetSecExp to 3 years or less & 4 years or more.	Correlation Coefficient	1.000	.478*
		Sig. (2-tailed)	.	.025
		N	22	22
	DummySecAssExp.13 Recode of SecAsseExp to 3 years or less & 4 years or more.	Correlation Coefficient	.478*	1.000
		Sig. (2-tailed)	.025	.
		N	22	22

*. Correlation is significant at the 0.05 level (2-tailed).

Table C9 Hypothesis Testing of the NetAdmin, NetSec, FISMA and SecAss Variables

Hypothesis Test Summary

	Null Hypothesis	Test	Sig.	Decision
1	The categories of 10. Net. Admin. Exp. occur with equal probabilities.	One-Sample Chi-Square Test	.823	Retain the null hypothesis.
2	The categories of 11. Net. Sec. Exp. occur with equal probabilities.	One-Sample Chi-Square Test	.059	Retain the null hypothesis.
3	The categories of 12. FISMA Exp. occur with equal probabilities.	One-Sample Chi-Square Test	.008	Reject the null hypothesis.
4	The categories of 13. Sec. Ass. Exp. occur with equal probabilities.	One-Sample Chi-Square Test	.008	Reject the null hypothesis.

Asymptotic significances are displayed. The significance level is .05.

Table C10 Dummy of SecAss and NetAdmin Experience

			DummySecAssExp.13 Recode of SecAsseExp to 3 years or less & 4 years or more.	DummyNetAdminExp.10 Recode of NetworkAdminExp to 3 years or less & 4 years or more.
Spearman's rho	DummySecAssExp.13 Recode of SecAsseExp to 3 years or less & 4 years or more.	Correlation Coefficient	1.000	-.153
		Sig. (2-tailed)	.	.498
		N	22	22
	DummyNetAdminExp.10 Recode of NetworkAdminExp to 3 years or less & 4 years or more.	Correlation Coefficient	-.153	1.000
		Sig. (2-tailed)	.498	.
		N	22	22

Table C11 Inter-Item Correlation Matrix

	Net.Admin.Exp.10 10. Net. Admin. Exp.	Net.Sec.Exp.11 11. Net. Sec. Exp.	FISMAExp.12 12. FISMA Exp.	Sec.Ass.Exp.13 13. Sec. Ass. Exp.
Net.Admin.Exp.10 10. Net. Admin. Exp.	1.000	-.088	-.163	-.216
Net.Sec.Exp.11 11. Net. Sec. Exp.	-.088	1.000	.610	.610
FISMAExp.12 12. FISMA Exp.	-.163	.610	1.000	.928
Sec.Ass.Exp.13 13. Sec. Ass. Exp.	-.216	.610	.928	1.000

Table C12 Inter-Item Covariance Matrix

	Net.Admin.Exp.10 10. Net. Admin. Exp.	Net.Sec.Exp.11 11. Net. Sec. Exp.	FISMAExp.12 12. FISMA Exp.	Sec.Ass.Exp.13 13. Sec. Ass. Exp.
Net.Admin.Exp.10 10. Net. Admin. Exp.	1.206	-.082	-.145	-.193
Net.Sec.Exp.11 11. Net. Sec. Exp.	-.082	.719	.420	.420
FISMAExp.12 12. FISMA Exp.	-.145	.420	.660	.613
Sec.Ass.Exp.13 13. Sec. Ass. Exp.	-.193	.420	.613	.660

Table C13 Inter-Item Correlation Matrix

	Net.Admin.Exp.10 10. Net. Admin. Exp.	Net.Sec.Exp.11 11. Net. Sec. Exp.	FISMAExp.12 12. FISMA Exp.	Sec.Ass.Exp.13 13. Sec. Ass. Exp.
Net.Admin.Exp.10 10. Net. Admin. Exp.	1.000	-.088	-.163	-.216
Net.Sec.Exp.11 11. Net. Sec. Exp.	-.088	1.000	.610	.610
FISMAExp.12 12. FISMA Exp.	-.163	.610	1.000	.928
Sec.Ass.Exp.13 13. Sec. Ass. Exp.	-.216	.610	.928	1.000

Table C14 Inter-Item Covariance Matrix

	Net.Admin.Exp.10 10. Net. Admin. Exp.	Net.Sec.Exp.11 11. Net. Sec. Exp.	FISMAExp.12 12. FISMA Exp.	Sec.Ass.Exp.13 13. Sec. Ass. Exp.
Net.Admin.Exp.10 10. Net. Admin. Exp.	1.206	-.082	-.145	-.193
Net.Sec.Exp.11 11. Net. Sec. Exp.	-.082	.719	.420	.420
FISMAExp.12 12. FISMA Exp.	-.145	.420	.660	.613
Sec.Ass.Exp.13 13. Sec. Ass. Exp.	-.193	.420	.613	.660

Table C15 Cronbach's Alpha for the Data Collection Questionnaire

Sect.	Description & Item numbers	Valid Cases	# Items	Cronbach's α Coefficient
1	Yrs experience & other characteristics of the respondents (1 – 17)	22	4	**0.591**
2.1	Validate the information system breakdown structure. (18 – 26)	22	8	**0.911**
2.2	Validate the e-Government Technical Security Controls E-R Diagram (27 – 51)	22	20	**0.914**
3	Identify effective IA risk mitigation and management Strategies (52 – 88)	22	37	**0.913**
4	Duration, costs and security assessed organizations (89 – 94)	20	4	**0.740**

Table C17 Scale Ranking for Section 2 of the Questionnaire

		18. ISBS First Level Cat.	19. Computers Sub-Cat	20. Infrastructure Sub-Cat	21. PDA Sub-Cat	22. Imaging Sub-Cat	23. Other Sub-Cat	24. Generic Components	25. Use of ISBS
N	Valid	22	22	22	22	22	22	22	22
	Missing	0	0	0	0	0	0	0	0
Mean		3.23	3.18	3.18	3.23	3.27	3.14	3.23	3.36
Median		3.00	3.00	3.00	3.00	3.00	3.00	3.00	3.00
Mode		3	3	3	3[a]	4	3	3	3
Std. Deviation		.685	.733	.733	.752	.767	.834	.612	.581
Skewness		-.323	-.304	-1.103	-.413	-.529	-.816	-.142	-.212
Std. Error of Skewness		.491	.491	.491	.491	.491	.491	.491	.491
Kurtosis		-.697	-.973	2.628	-1.036	-1.042	.497	-.285	-.621
Std. Error of Kurtosis		.953	.953	.953	.953	.953	.953	.953	.953

a. Multiple modes exist. The smallest value is shown

Table C18. ISBS First Level Cat.

		Frequency	Percent	Valid Percent	Cumulative %
Valid	Disagree	3	13.6	13.6	13.6
	Agree	11	50.0	50.0	63.6
	Strongly Agree	8	36.4	36.4	100.0
	Total	22	100.0	100.0	

Table C19. Computers Sub-Cat

		Frequency	Percent	Valid Percent	Cumulative %
Valid	Disagree	4	18.2	18.2	18.2
	Agree	10	45.5	45.5	63.6
	Strongly Agree	8	36.4	36.4	100.0
	Total	22	100.0	100.0	

Table C20. Infrastructure Sub-Cat

		Frequency	Percent	Valid Percent	Cumulative %
Valid	Strongly Disagree	1	4.5	4.5	4.5
	Disagree	1	4.5	4.5	9.1
	Agree	13	59.1	59.1	68.2
	Strongly Agree	7	31.8	31.8	100.0
	Total	22	100.0	100.0	

Table C21. PDA Sub-Cat

		Frequency	Percent	Valid Percent	Cumulative %
Valid	Disagree	4	18.2	18.2	18.2
	Agree	9	40.9	40.9	59.1
	Strongly Agree	9	40.9	40.9	100.0
	Total	22	100.0	100.0	

Table C22. Imaging Sub-Cat

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Disagree	4	18.2	18.2	18.2
	Agree	8	36.4	36.4	54.5
	Strongly Agree	10	45.5	45.5	100.0
	Total	22	100.0	100.0	

Table C23. Other Sub-Cat

		Frequency	Percent	Valid Percent	Cumulative %
Valid	Strongly Disagree	1	4.5	4.5	4.5
	Disagree	3	13.6	13.6	18.2
	Agree	10	45.5	45.5	63.6
	Strongly Agree	8	36.4	36.4	100.0
	Total	22	100.0	100.0	

Table C24. Generic Components

		Frequency	Percent	Valid Percent	Cumulative %
Valid	Disagree	2	9.1	9.1	9.1
	Agree	13	59.1	59.1	68.2
	Strongly Agree	7	31.8	31.8	100.0
	Total	22	100.0	100.0	

Table C25. Use of ISBS

		Frequency	Percent	Valid Percent	Cumulative %
Valid	Disagree	1	4.5	4.5	4.5
	Agree	12	54.5	54.5	59.1
	Strongly Agree	9	40.9	40.9	100.0
	Total	22	100.0	100.0	

Table C26 Chi-Share Test for the ISBS Model

	Recode of ISBSFirstLevl Cat to agree and disagree.	Recode of ComputersSub Cat to agree and disagree.	Recode of InfrastructureS ubCat to agree and disagree.	Recode of PDASubCat to agree and disagree.	Recode of ImagingSubCat to agree and disagree.	Recode of OtherSubCat to agree and disagree.	Recode of GenericCompo nents to agree and disagree.	Recode of UseofISBS to agree and disagree.
Chi-square	11.636[a]	8.909[a]	14.727[a]	8.909[a]	8.909[a]	8.909[a]	14.727[a]	18.182[a]
df	1	1	1	1	1	1	1	1
Asymp. Sig.	.001	.003	.000	.003	.003	.003	.000	.000

a. 0 cells (.0%) have expected frequencies less than 5. The minimum expected cell frequency is 11.0.

Table C27. User unique ID

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Agree	5	22.7	22.7	22.7
	Strongly Agree	17	77.3	77.3	100.0
	Total	22	100.0	100.0	

Table C28. User Single ID

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Disagree	5	22.7	22.7	22.7
	Agree	8	36.4	36.4	59.1
	Strongly Agree	9	40.9	40.9	100.0
	Total	22	100.0	100.0	

Table C29. IA Multiple Users

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Agree	10	45.5	45.5	45.5
	Strongly Agree	12	54.5	54.5	100.0
	Total	22	100.0	100.0	

Table C30. IA no Users

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	1	4.5	4.5	4.5
	Disagree	2	9.1	9.1	13.6
	Agree	14	63.6	63.6	77.3
	Strongly Agree	5	22.7	22.7	100.0
	Total	22	100.0	100.0	

Table C32. A System unique ID

		Frequency	Percent	Valid Percent	Cumulative %
Valid	Agree	9	40.9	40.9	40.9
	Strongly Agree	13	59.1	59.1	100.0
	Total	22	100.0	100.0	

Table C33. System single ID

		Frequency	Percent	Valid Percent	Cumulative %
Valid	Disagree	3	13.6	13.6	13.6
	Agree	12	54.5	54.5	68.2
	Strongly Agree	7	31.8	31.8	100.0
	Total	22	100.0	100.0	

Table C34. IA multiple systems

		Frequency	Percent	Valid Percent	Cumulative %
Valid	Agree	10	45.5	45.5	45.5
	Strongly Agree	12	54.5	54.5	100.0
	Total	22	100.0	100.0	

Table C35. IA of no systems

		Frequency	Percent	Valid Percent	Cumulative %
Valid	Disagree	2	9.1	9.1	9.1
	Agree	11	50.0	50.0	59.1
	Strongly Agree	9	40.9	40.9	100.0
	Total	22	100.0	100.0	

Table C37. Authenticated IDs must access IS

		Frequency	Percent	Valid Percent	Cumulative %
Valid	Strongly Disagree	1	4.5	4.5	4.5
	Disagree	2	9.1	9.1	13.6
	Agree	9	40.9	40.9	54.5
	Strongly Agree	10	45.5	45.5	100.0
	Total	22	100.0	100.0	

Table C38. Authenticated IDs may access IS.

		Frequency	Percent	Valid Percent	Cumulative %
Valid	Strongly Disagree	1	4.5	4.5	4.5
	Disagree	1	4.5	4.5	9.1
	Agree	12	54.5	54.5	63.6
	Strongly Agree	8	36.4	36.4	100.0
	Total	22	100.0	100.0	

Table C39. AC controls an authenticated ID.

		Frequency	Percent	Valid Percent	Cumulative %
Valid	Strongly Disagree	1	4.5	4.5	4.5
	Disagree	1	4.5	4.5	9.1
	Agree	10	45.5	45.5	54.5
	Strongly Agree	10	45.5	45.5	100.0
	Total	22	100.0	100.0	

Table C40. AC multiple authenticated IDs.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Agree	9	40.9	40.9	40.9
	Strongly Agree	13	59.1	59.1	100.0
	Total	22	100.0	100.0	

Table C42. AC creates audit record

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Agree	8	36.4	36.4	36.4
	Strongly Agree	14	63.6	63.6	100.0
	Total	22	100.0	100.0	

Table C43. AC creates multiple audit records.

		Frequency	Percent	Valid Percent	Cumulative %
Valid	Agree	11	50.0	50.0	50.0
	Strongly Agree	11	50.0	50.0	100.0
	Total	22	100.0	100.0	

Table C44. AU audits an AC

		Frequency	Percent	Valid Percent	Cumulative %
Valid	Disagree	1	4.5	4.5	4.5
	Agree	9	40.9	40.9	45.5
	Strongly Agree	12	54.5	54.5	100.0
	Total	22	100.0	100.0	

Table C45. AU audits multiple AC

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Agree	11	50.0	50.0	50.0
	Strongly Agree	11	50.0	50.0	100.0
	Total	22	100.0	100.0	

Table C47. AU to a SC

		Frequency	Percent	Valid Percent	Cumulative %
Valid	Disagree	2	9.1	9.1	9.1
	Agree	9	40.9	40.9	50.0
	Strongly Agree	11	50.0	50.0	100.0
	Total	22	100.0	100.0	

Table C48. AU to multiple SC

		Frequency	Percent	Valid Percent	Cumulative %
Valid	Disagree	2	9.1	9.1	9.1
	Agree	12	54.5	54.5	63.6
	Strongly Agree	8	36.4	36.4	100.0
	Total	22	100.0	100.0	

Table C49. SC monitors an AU

		Frequency	Percent	Valid Percent	Cumulative %
Valid	Disagree	1	4.5	4.5	4.5
	Agree	10	45.5	45.5	50.0
	Strongly Agree	11	50.0	50.0	100.0
	Total	22	100.0	100.0	

Table C50. SC monitor multiple AU

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Disagree	1	4.5	4.5	4.5
	Agree	12	54.5	54.5	59.1
	Strongly Agree	9	40.9	40.9	100.0
	Total	22	100.0	100.0	

Table C51 Analysis of the e-Government Relational Technical Controls

	27. User unique ID	28. User Single ID	29. IA Multiple Users	30. IA no Users	32. A System unique ID	33. System single ID	34. IA multiple systems	35. IA of no systems	37. Authenticated IDs must access IS	38. Authenticated IDs may access IS.	39. AC controls an authenticated ID.	40. AC multiple authenticated IDs.	42. AC creates audit record	43. AC creates multiple audit records.	44. AU audits an AC	45. AU audits multiple AC	47. AU to a SC	48. AU to multiple SC	49. SC monitors an AU	50. SC monitor multiple AU
Valid	22.00	22.00	22.00	22.00	22.00	22.00	22.00	22.00	22.00	22.00	22.00	22.00	22.00	22.00	22.00	22.00	22.00	22.00	22.00	22.00
Missing	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Mean	**3.77**	3.18	3.55	3.05	3.59	3.18	3.55	3.32	3.27	3.23	3.32	3.59	3.64	3.50	3.50	3.50	3.41	3.27	3.45	3.36
Median	4.00	3.00	4.00	3.00	4.00	3.00	4.00	3.00	3.00	3.00	3.00	4.00	4.00	3.50	4.00	3.50	3.50	3.00	3.50	3.00
Mode	4.00	4.00	4.00	3.00	4.00	3.00	4.00	3.00	4.00	3.00	3a	4.00	4.00	3a	4.00	3a	4.00	3.00	4.00	3.00
Std. Deviation	0.43	0.80	0.51	0.72	0.50	0.66	0.51	0.65	0.83	0.75	0.78	0.50	0.49	0.51	0.60	0.51	0.67	0.63	0.60	0.58
Variance	0.18	0.63	0.26	0.52	0.25	0.44	0.26	0.42	0.68	0.57	0.61	0.25	0.24	0.26	0.36	0.26	0.44	0.40	0.36	0.34
Skewness	-1.40	-0.35	-0.20	-0.90	-0.40	-0.21	-0.20	-0.40	-1.13	-1.15	-1.31	-0.40	-0.61	0.00	-0.74	0.00	-0.70	-0.27	-0.55	-0.21
Std. Error of Skewness	0.49	0.49	0.49	0.49	0.49	0.49	0.49	0.49	0.49	0.49	0.49	0.49	0.49	0.49	0.49	0.49	0.49	0.49	0.49	0.49
Kurtosis	-0.06	-1.29	-2.17	2.12	-2.04	-0.55	-2.17	-0.54	1.23	2.43	2.37	-2.04	-1.80	-2.21	-0.31	-2.21	-0.43	-0.46	-0.52	-0.62
Std. Error of Kurtosis	0.95	0.95	0.95	0.95	0.95	0.95	0.95	0.95	0.95	0.95	0.95	0.95	0.95	0.95	0.95	0.95	0.95	0.95	0.95	0.95
Range	1.00	2.00	1.00	3.00	1.00	2.00	1.00	2.00	3.00	3.00	3.00	1.00	1.00	1.00	2.00	1.00	2.00	2.00	2.00	2.00
a. Multiple modes exist. The smallest value is shown																				

Table C52 Analysis of the e-Government Relational Technical Controls

	Recode of UserSingle to agree and disagree.	Recode of IAnoUses to agree and disagree.	Recode of SystemSingleID to agree and disagree.	Recode of IAofNOSystems to agree and disagree.	Recode of AuthenticatedIDsmustaccessIS to agree and disagree.	Recode of AuthenticatedIDsmayaccessIS to agree and disagree.	Recode of ACcontrolsanAuthenticatedID to agree and disagree.	Recode of AUauditsanAC to agree and disagree.	Recode of AUtoSC to agree and disagree.	Recode of AUtoMultipleSC to agree and disagree.	Recode of SCMonitorsanAU to agree and disagree.	Recode of SCmonitormultipleAU to agree and disagree.
Chi-square	6.545[a]	11.636[a]	11.636[a]	14.727[a]	11.636[a]	14.727[a]	14.727[a]	18.182[a]	14.727[a]	14.727[a]	18.182[a]	18.182[a]
df	1	1	1	1	1	1	1	1	1	1	1	1
Asymp. Sig.	.011	.001	.001	.000	.001	.000	.000	.000	.000	.000	.000	.000

a. 0 cells (.0%) have expected frequencies less than 5. The minimum expected cell frequency is 11.0.

Table C53 IA-2 Analysis

	52. IA-2: Authenticated user IDs access IS	53. IA-2: IA manage ID generator for IS	54. IA-2: ID & AC integrated for apps & IS access	55. IA-2: Multi-factor authen. increases IS security posture	56. IA-2: ID generators multi-factor authen. capable.	authent provided by a separate device from IS.	synchronous/challenge-response one-time authenticators.
Valid	22	22	22	22	22	22	22
Missing	0	0	0	0	0	0	0
Mean	3.36	3.36	3.5	3.5	3.41	3.5	3.45
Median	3	3	3.5	4	3	4	3
Mode	3	3	3a	4	3	4	3
Std. Deviation	0.581	0.492	0.512	0.598	0.59	0.598	0.51
Variance	0.338	0.242	0.262	0.357	0.348	0.357	0.26
Skewness	-0.212	0.609	0	-0.736	-0.379	-0.736	0.196
Std. Error of Skewness	0.491	0.491	0.491	0.491	0.491	0.491	0.491
Kurtosis	-0.621	-1.802	-2.211	-0.312	-0.626	-0.312	-2.168
Std. Error of Kurtosis	0.953	0.953	0.953	0.953	0.953	0.953	0.953
Range	2	1	1	2	2	2	1

Table C54 IA-3 & IA-4 Analysis

	60. IA-3: Centrally manage System/device ids	61. IA-3: Using MAC addresses for device/system IA	62. IA-3: Using of IP addresses for IA of devices/systems	63. IA-3: Using bidirectional authentication for devices		65. IA-4: Uniquely identify users, processes, systems and devices	66. IA-4: Prevent reuse of user, process, system or device identifiers	67. IA-4: Disabling user identifier after an organization period of inactivity	68. IA-4: Using user identifiers not matching email address
Valid	22	22	22	22		22	22	22	22
Missing	0	0	0	0		0	0	0	0
Mean	3.32	3.05	3.09	3.45		3.68	3.23	3.41	3.27
Median	3	3	3	3		4	3	3	3
Mode	3	3	3	3		4	3	3	3
Std. Deviation	0.646	0.722	0.75	0.51		0.477	0.685	0.503	0.631
Variance	0.418	0.522	0.563	0.26		0.227	0.47	0.253	0.398
Skewness	-0.404	-0.069	-0.898	0.196		-0.839	-0.323	0.397	-0.269
Std. Error of Skewness	0.491	0.491	0.491	0.491		0.491	0.491	0.491	0.491
Kurtosis	-0.54	-0.929	1.733	-2.168		-1.436	-0.697	-2.037	-0.463
Std. Error of Kurtosis	0.953	0.953	0.953	0.953		0.953	0.953	0.953	0.953
Range	2	2	3	1		1	2	1	2
a. Multiple modes exist. The smallest value is shown									

Table C55 IA-5 Analysis

	70. IA-5: Limiting the reuse of authenticators for users/processes	71. IA-5: Limiting the reuse of authenticators for systems/devices	72. IA-5: Minimum period before requiring a password change	73. IA-5: Maximum period before requiring a password change	74. IA-5: Automated tools to determine the strength of authenticators to resist attacks.	75. IA-5: Different unique authenticators (or passwords) for different IS	76. IA-5: Single sign-on improves the security posture of IS.	77. IA-5: One-time passwords	78. IA-5: Restricting the number of accounts individuals have on multiple IS
Valid	22	22	22	22	22	22	22	22	22
Missing	0	0	0	0	0	0	0	0	0
Mean	3.45	3.41	3.32	3.45	3.55	3.27	3.05	3.18	3.27
Median	3.5	3	3	3	4	3	3	3	3
Mode	4	3	3	3	4	3	4	3	3
Std. Deviation	0.596	0.503	0.568	0.51	0.596	0.703	0.844	0.733	0.631
Variance	0.355	0.253	0.323	0.26	0.355	0.494	0.712	0.537	0.398
Skewness	-0.553	0.397	-0.05	0.196	-0.933	-0.442	-0.091	-0.304	-0.269
Std. Error of Skewness	0.491	0.491	0.491	0.491	0.491	0.491	0.491	0.491	0.491
Kurtosis	-0.524	-2.037	-0.506	-2.168	0.025	-0.762	-1.606	-0.973	-0.463
Std. Error of Kurtosis	0.953	0.953	0.953	0.953	0.953	0.953	0.953	0.953	0.953
Range	2	1	2	1	2	2	2	2	2
a. Multiple modes exist. The smallest value is shown									

Table C56 IA-4 to IA-8 Analysis

	79. IA-4: Period of inactivity (days) before disabling a user account	80. IA-5: Frequence (days) for changing / refreshing authenticators (or passwords)		81. IA-5: Quantity of user password histories remember and prevent reusing.	82. IA-5: Minimum number of characters for passwords		85. IA-6: Obscuring of feedback during IA	86. IA-7: The use of cryptographic modules during IA	of non-organizational users improves the security posture of the information system.
Valid	22	22		22	22		22	22	22
Missing	0	0		0	0		0	0	0
Mean	2.68	2.64		2.27	2.23		3.41	3.64	3.32
Median	3	3		2	2		3	4	3
Mode	3	3		2	2		3	4	3
Std. Deviation	1.129	0.953		1.12	0.813		0.59	0.492	0.568
Variance	1.275	0.909		1.255	0.66		0.348	0.242	0.323
Skewness	0.483	0.114		0.521	0.712		-0.379	-0.609	-0.05
Std. Error of Skewness	0.491	0.491		0.491	0.491		0.491	0.491	0.491
Kurtosis	0.006	0.908		-1.033	0.595		-0.626	-1.802	-0.506
Std. Error of Kurtosis	0.953	0.953		0.953	0.953		0.953	0.953	0.953
Range	4	4		3	3		2	1	2
a. Multiple modes exist. The smallest value is shown									

Table C57 Password Characteristics Analysis (Items 83 of the questionnaire)

	83i. Passwords case sensitive	83ii. Passwords exceed certain number of characters	83iii. Using of upper & lower cases	83iv. Using numbers	83v. Using special characters	83vi. Minimum requirement for each item
Valid	22	22	22	22	22	22
Missing	0	0	0	0	0	0
Mean	0.95	1	0.91	1	0.91	0.68
Median	1	1	1	1	1	1
Mode	1	1	1	1	1	1
Std. Deviation	0.213	0	0.294	0	0.294	0.477
Variance	0.045	0	0.087	0	0.087	0.227
Skewness	-4.69		-3.059		-3.059	-0.839
Std. Error of Skewness	0.491	0.491	0.491	0.491	0.491	0.491
Kurtosis	22		8.085		8.085	-1.436
Std. Error of Kurtosis	0.953	0.953	0.953	0.953	0.953	0.953
Range	1	0	1	0	1	1
a. Multiple modes exist. The smallest value is shown						

Table C58 Chi-Square Calculations for Section 3 of the Questionnaire

	Recode of IA2AuthenticatedUsersIDaccessIS to agree and disagree.	Recode of 55 to agree and disagree.	Recode of 56 to agree and disagree.	Recode of 57 to agree and disagree.	Recode of 60 to agree and disagree.	Recode of 61 to agree and disagree.	Recode of 62 to agree and disagree.	Recode of 66 to agree and disagree.	Recode of 68 to agree and disagree.
Chi-square	18.182a	18.182a	18.182a	18.182a	14.727a	6.545a	11.636a	11.636a	14.727a
df	1	1	1	1	1	1	1	1	1
Asymp. Sig.	0	0	0	0	0	0.011	0.001	0.001	0
a. 0 cells (.0%) have expected frequencies less than 5. The minimum expected cell frequency is 11.0.									

	Recode of 70 to agree and disagree.	Recode of 72 to agree and disagree.	Recode of 74 to agree and disagree.	Recode of 75 to agree and disagree.	Recode of 76 to agree and disagree.	Recode of 77 to agree and disagree.	Recode of 78 to agree and disagree.	Recode of 85 to agree and disagree.	Recode of 87 to agree and disagree.
Chi-square	18.182a	18.182a	18.182a	11.636a	2.909a	8.909a	14.727a	18.182a	18.182a
df	1	1	1	1	1	1	1	1	1
Asymp. Sig.	0	0	0	0.001	0.088	0.003	0	0	0
a. 0 cells (.0%) have expected frequencies less than 5. The minimum expected cell frequency is 11.0.									

Table C59 Hypothesis tests for the questionnaire items.

Item #	Null Hypothesis	Chi-square	df	Asymp. Sig.	Nonparametric Test	Sig.	Comments
18	There is no significance between the respondents that agree or disagree to the statement that 'The sub-categories (computers, network infrastructure, personal digital assistants, imaging device and other devices) identified in Figure 1.0 are sufficient to categorize all information systems.'	11.636[a]	1	0.001	One-Sample Binomial Test	.001	Reject the null hypothesis
19	There is no significance between the respondents that agree or disagree to the statement that 'The components identified for the computers sub-category are sufficient to identify information systems for this sub-category.'	8.909[a]	1	0.003	One-Sample Binomial Test	.004	Reject the null hypothesis
20	There is no significance between the respondents that agree or disagree to the statement that 'The components identified for the network infrastructure sub-category are sufficient to identify information systems for this sub-category.'	14.727[a]	1	0	One-Sample Binomial Test	.000	Reject the null hypothesis
21	There is no significance between the respondents that agree or disagree to the statement that 'The components identified for the personal digital assistants sub-category are sufficient to identify information systems for this sub-category.'	8.909[a]	1	0.003	One-Sample Binomial Test	.004	Reject the null hypothesis
22	There is no significance between the respondents that agree or disagree to the statement that 'The components identified for the imaging devices sub-category are sufficient to identify information systems for this sub-category.'	8.909[a]	1	0.003	One-Sample Binomial Test	.004	Reject the null hypothesis

Item #	Null Hypothesis	Chi-square	df	Asymp. Sig.	Nonparametric Test	Sig.	Comments
23	There is no significance between the respondents that agree or disagree to the statement that 'The components identified for the other devices sub-category are a sufficient catch-all for information systems not identified in the computers, network infrastructure, personal digital assistants and imaging devices sub-categories.'	8.909[a]	1	0.003	One-Sample Binomial Test	.004	Reject the null hypothesis
24	There is no significance between the respondents that agree or disagree to the statement that 'The generic sub-components identified for the different components are sufficient to assess risks at the sub-component levels. '	14.727[a]	1	0	One-Sample Binomial Test	.000	Reject the null hypothesis
25	There is no significance between the respondents that agree or disagree to the statement that 'The use of an information system breakdown structure improves the ability of assessors to identify organizational information system assets. '	18.182[a]	1	0	One-Sample Binomial Test	.000	Reject the null hypothesis
27	There is no significance between the respondents that agree or disagree to the statement that 'Each Users/Processes should have a unique identifier for authentication to an information system.'	-	-	-	-	-	This variable is a constant. Chi-Square Test cannot be performed
28	There is no significance between the respondents that agree or disagree to the statement that 'Users/Processes should be restricted	6.565	1	.011	One-Sample Binomial Test	.017	Reject the null

Item #	Null Hypothesis	Chi-square	df	Asymp. Sig.	Nonparametric Test	Sig.	Comments
	to a single user/process id.'						hypothesis
29	There is no significance between the respondents that agree or disagree to the statement that 'An IA entity should be capable of identification and authentication of multiple users/processes.'	-	-	-	-	-	This variable is a constant. Chi-Square Test cannot be performed
30	There is no significance between the respondents that agree or disagree to the statement that 'An IA entity can exist that does not identify and authenticate users/process. (They may identify and authenticate only systems/devices)'	11.636	1	.001	One-Sample Binomial Test	.001	Reject the null hypothesis
32	There is no significance between the respondents that agree or disagree to the statement that 'A System/Device should have a unique identifier for authentication to an information system.'	-	-	-	-	-	This variable is a constant. Chi-Square Test cannot be performed

Item #	Null Hypothesis	Chi-square	df	Asymp. Sig.	Nonparametric Test	Sig.	Comments
33	There is no significance between the respondents that agree or disagree to the statement that 'A System/Device should be restricted to a single system/device id.'	11.363	1	.001	One-Sample Binomial Test	.001	Reject the null hypothesis
34	There is no significance between the respondents that agree or disagree to the statement that 'An IA entity should be capable of identification and authentication of multiple systems/devices. '	-	-	-	-	-	This variable is a constant. Chi-Square Test cannot be performed
35	There is no significance between the respondents that agree or disagree to the statement that 'An IA entity can exist that does not identify and authenticate systems/devices (They may identify and authenticate only Users/Processes)'	14.727	1	.000	One-Sample Binomial Test	.000	Reject the null hypothesis
37	There is no significance between the respondents that agree or disagree to the statement that 'Authenticated identifiers must be granted access to an information system.'	11.636	1	.001	One-Sample Binomial Test	0.001	Reject the null hypothesis
38	There is no significance between the respondents that agree or disagree to the statement that 'Authenticated identifiers may be granted access to multiple information systems.'	14.727	1	.000	One-Sample Binomial Test	0.001	Reject the null hypothesis

Item #	Null Hypothesis	Chi-square	df	Asymp. Sig.	Nonparametric Test	Sig.	Comments
39	There is no significance between the respondents that agree or disagree to the statement that 'The access control entity should control the access of at least one authenticated identifier. '	14.727	1	.001	One-Sample Binomial Test	0.001	Reject the null hypothesis
40	There is no significance between the respondents that agree or disagree to the statement that 'The access control entity should be capable of managing the access of multiple authenticated identifiers.'	-	-	-	-	-	This variable is a constant. Chi-Square Test cannot be performed
42	There is no significance between the respondents that agree or disagree to the statement that 'The access control entity must create an audit event record.'	-	-	-	-	-	This variable is a constant. Chi-Square Test cannot be performed

Item #	Null Hypothesis	Chi-square	df	Asymp. Sig.	Nonparametric Test	Sig.	Comments
43	There is no significance between the respondents that agree or disagree to the statement that 'The access control entity may create multiple audit events.'	-	-	-	-	-	This variable is a constant. Chi-Square Test cannot be performed
44	There is no significance between the respondents that agree or disagree to the statement that 'The audit and accountability entity must audit an access control entity.'	18.182	1	.000	One-Sample Binomial Test	0.000	Reject the null hypothesis.
45	There is no significance between the respondents that agree or disagree to the statement that 'The audit and accountability entity may audit multiple access control entities.'	-	-	-	-	-	This variable is a constant. Chi-Square Test cannot be performed
47	There is no significance between the respondents that agree or disagree to the statement that 'The audit and accountability entity should feed to a system and communication protection entity. '	14.727	1	.000	One-Sample Binomial Test	0.000	Reject the null hypothesis.

Item #	Null Hypothesis	Chi-square	df	Asymp. Sig.	Nonparametric Test	Sig.	Comments
48	There is no significance between the respondents that agree or disagree to the statement that 'The audit and accountability entity may feed to multiple systems and communication protection entities.'	14.727	1	.000	One-Sample Binomial Test	0.000	Reject the null hypothesis.
49	There is no significance between the respondents that agree or disagree to the statement that 'The system and communication protection entity must monitor an audit entity.'	18.182	1	.000	One-Sample Binomial Test	0.000	Reject the null hypothesis.
50	There is no significance between the respondents that agree or disagree to the statement that 'The system and communication protection entity may monitor multiple audit entities. '	18.182	1	.000	One-Sample Binomial Test	0.000	Reject the null hypothesis.
52	There is no significance between the respondents that agree or disagree to the statement that 'IA-2: Authenticated user/process IDs should be granted access to the information system.'	18.182	1	.000	One-Sample Binomial Test	.000	Reject the null hypothesis
53	There is no significance between the respondents that agree or disagree to the statement that 'IA-2: The identification and authentication control family should be use to manage identifier generator for an information system.'	-	-	-	-	-	This variable is a constant. Chi-Square Test cannot be performed

Item #	Null Hypothesis	Chi-square	df	Asymp. Sig.	Nonparametric Test	Sig.	Comments
54	There is no significance between the respondents that agree or disagree to the statement that 'IA-2: The identifier management and the access control entities, should be integrated for managing access to applications (residing on the information system)and the information system. '	-	-	-	-	-	This variable is a constant. Chi-Square Test cannot be performed
55	There is no significance between the respondents that agree or disagree to the statement that 'IA-2: The use of multi-factor authentication increases the security posture of information systems.'	18.182	1	.000	One-Sample Binomial Test	.000	Reject the null hypothesis
56	There is no significance between the respondents that agree or disagree to the statement that 'IA-2: Identifier generators should be capable of multi-factor authentication.'	18.182	1	.000	One-Sample Binomial Test	.000	Reject the null hypothesis
57	There is no significance between the respondents that agree or disagree to the statement that 'IA-2: Having one of the factors of multi-factor authentication provided by a device separate from the information system being access, improves the security posture of the information system. '	18.182	1	.000	One-Sample Binomial Test	.000	Reject the null hypothesis

Item #	Null Hypothesis	Chi-square	df	Asymp. Sig.	Nonparametric Test	Sig.	Comments
58	There is no significance between the respondents that agree or disagree to the statement that 'IA-2: The use of time synchronous or challenge-response one-time authenticators improves the security posture of information systems.'	-	-	-	-	-	This variable is a constant. Chi-Square Test cannot be performed
60	There is no significance between the respondents that agree or disagree to the statement that 'IA-3: System/device ids that should be centrally manage by an information system.'	14.727	1	.000	One-Sample Binomial Test	.000	Reject the null hypothesis
61	There is no significance between the respondents that agree or disagree to the statement that 'IA-3: The use of MAC addresses for the identification and authentication of devices/systems improves the security posture of an information system.'	6.545	1	0.011	One-Sample Binomial Test	.017	Reject the null hypothesis
62	There is no significance between the respondents that agree or disagree to the statement that 'IA-3: The use of IP addresses for identification and authentication of devices/systems improves the security posture of an information system.'	11.636	1	0.001	One-Sample Binomial Test	.001	Reject the null hypothesis

Item #	Null Hypothesis	Chi-square	df	Asymp. Sig.	Nonparametric Test	Sig.	Comments
63	There is no significance between the respondents that agree or disagree to the statement that 'IA-3: The use of bidirectional authentication between devices improves the security posture of an information system.'	-	-	-	-	-	This variable is a constant. Chi-Square Test cannot be performed
65	There is no significance between the respondents that agree or disagree to the statement that 'IA-4: Users, processes, systems and devices must be uniquely identified to an information system.'	-	-	-	-	-	This variable is a constant. Chi-Square Test cannot be performed
66	There is no significance between the respondents that agree or disagree to the statement that 'IA-4: Preventing the reuse of user, process, system or device identifiers increases the security posture of an information system.'	11.636	1	0.001	One-Sample Binomial Test	.001	Reject the null hypothesis

Item #	Null Hypothesis	Chi-square	df	Asymp. Sig.	Nonparametric Test	Sig.	Comments
67	There is no significance between the respondents that agree or disagree to the statement that 'IA-4: Disabling user identifier after an organization defined period of inactivity improves the security posture of an information system.'	-	-	-	-	-	This variable is a constant. Chi-Square Test cannot be performed
68	There is no significance between the respondents that agree or disagree to the statement that 'IA-4: The use of user identifiers that do not match the email address of users improves the security posture of an information system.'	14.727	1	.000	One-Sample Binomial Test	.000	Reject the null hypothesis
70	There is no significance between the respondents that agree or disagree to the statement that 'IA-5: Limiting the reuse of authenticators for users/processes improves the security posture of information systems'	18.182	1	.000	One-Sample Binomial Test	.000	Reject the null hypothesis
71	There is no significance between the respondents that agree or disagree to the statement that 'IA-5: Limiting the reuse of authenticators for systems/devices improves the security posture of information systems'	-	-	-	-	-	This variable is a constant. Chi-Square Test cannot be performed

Item #	Null Hypothesis	Chi-square	df	Asymp. Sig.	Nonparametric Test	Sig.	Comments
72	There is no significance between the respondents that agree or disagree to the statement that 'IA-5: Establishing the minimum period before requiring a password change improves the security posture of information systems.'	18.182	1	.000	One-Sample Binomial Test	.000	Reject the null hypothesis
73	There is no significance between the respondents that agree or disagree to the statement that 'IA-5: Establishing the maximum period before requiring a password change improves the security posture of information systems.'	-	-	-	-	-	This variable is a constant. Chi-Square Test cannot be performed
74	There is no significance between the respondents that agree or disagree to the statement that 'IA-5: The use of automated tools to determine the strength of authenticators to resist attacks improves the security posture of information system.'	18.182	1	.000	One-Sample Binomial Test	.000	Reject the null hypothesis
75	There is no significance between the respondents that agree or disagree to the statement that 'IA-5: The use of different unique authenticators (or passwords) for different information systems improves the security posture of the organization.'	11.636	1	0.001	One-Sample Binomial Test	.001	Reject the null hypothesis
76	There is no significance between the respondents that agree or disagree to the statement that 'IA-5: Employing the use of single sign-on improves the security posture of information systems.'	2.909	1	0.088	One-Sample Binomial Test	.134	Retain the null hypothesis

Item #	Null Hypothesis	Chi-square	df	Asymp. Sig.	Nonparametric Test	Sig.	Comments
77	There is no significance between the respondents that agree or disagree to the statement that 'IA-5: Using one-time passwords improves the security posture of information systems.'	8.909	1	0.003	One-Sample Binomial Test	.004	Reject the null hypothesis
78	There is no significance between the respondents that agree or disagree to the statement that 'IA-5: Restricting the number of accounts individuals have on multiple information systems improves their security posture.'	14.727	1	.000	One-Sample Binomial Test	.000	Reject the null hypothesis
79	The categories of the period of inactivity before a user account is disabled occurs with equal probabilities	7.545	4	0.110	One-Sample Chi-Square Test	.110	Retain the null hypothesis
80	The categories of the period before authenticators are changed/refreshed occur with equal probabilities	18.909	4	.001	One-Sample Chi-Square Test	.001	Reject the null hypothesis. 61-90 days is significant
81	The categories of how many password histories the information system should prevent users from reusing occurs with equal probabilities	4.545	3	.208	One-Sample Chi-Square Test	.208	Retain the null hypothesis
82	The categories for the minimum number of characters for passwords occur with equal probabilities.	14	3	.003	One-Sample Chi-Square Test	.003	Reject the null hypothesis

Item #	Null Hypothesis	Chi-square	df	Asymp. Sig.	Nonparametric Test	Sig.	Comments
83i	The categories for requiring passwords to be case sensitive occurs with equal probabilities	18.182	1	.000			Reject the null hypothesis
83ii	The categories for requiring that the password exceeds a certain number of characters occurs with equal probabilities	-	-	-	-	-	This variable is constant. Chi-Square Test cannot be performed.
83iii	The categories for requiring both upper and lower case letters occurs with equal probabilities	14.727	1	.000			Reject the null hypothesis
83iv	The categories for requiring the use of numbers in passwords occurs with equal probabilities	-	-	-	-	-	This variable is constant. Chi-Square Test cannot be performed.

Item #	Null Hypothesis	Chi-square	df	Asymp. Sig.	Nonparametric Test	Sig.	Comments
83v	The categories for requiring the use of special characters in passwords occurs with equal probabilities	14.727	1	.000			Reject the null hypothesis
83vi	The categories for requiring a minimum requirement for each of the items in (83) occurs with equal probabilities.	2.909	1	.088			Retain the null hypothesis
85	There is no significance between the respondents that agree or disagree to the statement that 'IA-6: Obscuring of feedback during authentication improves the security posture of information systems.'	18.182	1	.000	One-Sample Binomial Test	.000	Reject the null hypothesis
86	There is no significance between the respondents that agree or disagree to the statement that 'IA-7: The use of cryptographic modules during authentication improves the security posture of information systems.'	-	-	-	-	-	This variable is constant. Chi-Square Test cannot be performed.
87	There is no significance between the respondents that agree or disagree to the statement that 'IA-8: The identification and authentication of non-organizational users improves the security posture of the information system.'	18.182	1	.000			Reject the null hypothesis

Table C60 Bayesian Probability Calculation for the duration of the different tasks

				Probabilities of Tasks			
Range	**Max**	**Min**	**Median**	**Assess Docs.**	**Interviewing**	**Testing**	**Reporting**
<=1	1	0	0.5	5.00%	15.00%	15.00%	5.00%
2-3	3	2	2.5	35.00%	30.00%	35.00%	20.00%
4-5	5	4	4.5	20.00%	20.00%	20.00%	25.00%
6-7	7	6	6.5	15.00%	35.00%	25.00%	30.00%
>=8	8	8	8	25.00%	0.00%	5.00%	20.00%

Max Docs. Ass.	**Max Interview**	**Max Testing**	**Max Reporting**
0.05	0.15	0.15	0.05
1.05	0.9	1.05	0.6
1	1	1	1.25
1.05	2.45	1.75	2.1
2	0	0.4	1.6
5.15	**4.5**	**4.35**	**5.6**

Min Docs. Ass.	**Min Interview**	**Min Testing**	**Min Reporting**
0	0	0	0
0.7	0.6	0.7	0.4
0.8	0.8	0.8	1
0.9	2.1	1.5	1.8
2	0	0.4	1.6
4.4	**3.5**	**3.4**	**4.8**

Median Docs. Ass.	**Median Interview**	**Median Testing**	**Median Reporting**
0.025	0.075	0.075	0.025
0.875	0.75	0.875	0.5
0.9	0.9	0.9	1.125
0.975	2.275	1.625	1.95
2	0	0.4	1.6
4.775	**4**	**3.875**	**5.2**

Table C61 Pilot Questionnaire Changes

Ques #	Previous	Change To
Que. 8.	How would you classify yourself? (Select one) ☐ Project Manager ☐ Information Security Contractor ☐ Network Engineer ☐ Network Administrator ☐ Other:	8. How would you classify yourself? (Select all that apply) ☐ Project Manager ☐ Information Security Contractor ☐ Network Engineer ☐ Network Administrator ☐ Other:
Que. 16-i	16-i. What is your highest level of education? ☐ High School Diploma ☐ Associate Degree ☐ Bachelors Degree ☐ Masters Degree ☐ PhD ☐ Post Graduate ☐ Other	What is your highest level of education? (Select all that apply) ☐ High School Diploma ☐ Associate Degree ☐ Bachelors Degree ☐ Masters Degree ☑ PhD ☑ Post Graduate ☐ Other
Feedback Questions	Please provide any additional feedback in the space below.	Kindly provide additional feedback for items you disagree or strongly disagree with.
Que. 94	Please provide any additional feedback in the space below.	Kindly provide additional feedback for durations greater than or equal to 8 days.
Feedback for Ques. 89 – 92	Maximum duration was >=8 hrs.	For durations greater than 8 hours please specify what the duration should be and why.
Que. 94	What is the fee (in $/hr) information assurance organizations charge for	What is the fee (in $/hr) information assurance organizations charge customers for performing

Ques #	Previous	Change To
	performing security assessments?	security assessment of their systems?
Formatting	Some blank pages exist in the Word 97-2003 Version of the questionnaire.	The blank pages have been removed and reformatted to be consistent with the Word 2007 version of the questionnaire.
Que. 10	10. Experience in the information technology related field (in years)	This item was removed from the questionnaire as it was a given that the respondents had to have extensive experience with information assurance for them to be included in the research. The remaining questions were renumbered.
Que. 11.	Experience in the network administration related field (in years)	Change to question 10 and a forced response with option buttons and duration in ranges. Years of experience in the network administrator related field (Select one) ☐ <= 3 ☐ 4 - 8 ☐ 9 - 13 ☐ >= 14
Que. 12	Experience in the network security related field (in years)	Change to question 11 and a forced response with option buttons and duration in ranges. Years experience in the network security related field (Select one) ☐ <= 3 ☐ 4 - 8 ☐ 9 - 13 ☐ >= 14

Ques #	Previous	Change To
Que. 13	Experience with FISMA e-Government implementation related field (in years)	Change to question 12 and a forced response with option buttons and duration in ranges. Years experience in the FISMA e-Government implementation related field (years) ○ <= 3 ○ 4 - 8 ○ 9 - 13 ○ >= 14
Que. 60.	IA-3: System/device ids that should be centrally manage by an information system.	IA-3: System/device ids should be centrally managed by an information system.
Ques 79 & 80	<= 30, 30 - 60, 60 - 90, 90 - 120, >=120	<= 30, 31 - 60, 61 - 90, 91 - 120, >=121
Que. 83.	IA-5: Select the options that you believe improves the security of authenticators.	IA-5: Select the options that you believe improves the security of authenticators. (Select all that apply)

Table C62 Hierarchical e-Government Model vs Relational e-Government Model

Item	Hierarchical e-Government Model	Relational e-Government Model
1.	This model takes a hierarchical directory approach to identify the security controls	This model uses a relational approach to identify the security control
2.	It does not consider the relationships between the controls	It considers the relationships between the controls
3.	It has duplicates in the security controls & causes data/information integrity issues.	It does not permit duplicates for the security controls, or their attributes thereby improving data integrity
4.	There tends to be a lot of duplicates between the controls	It reduces the likelihood of having duplicate controls
5.	It is impossible to automate the workflow	The workflow process can be automated
6.	There is no way to track the progress of a security assessment	It can provide real-time tracking of the progress of a security assessment
8.	The integration of data/information and templates is tightly coupled and it does not allow for the reuse or real-time update of information and documentation	The data/information is not restricted to a single document template and it allows for the reuse of information and the cascading up of updates
9.	The work involved is repetitive and tedious	It drastically reduces the drudgery involved in performing security assessment
10.	It does not allow for the pre-identification or	It allows for the pre-identification and easy

Item	Hierarchical e-Government Model	Relational e-Government Model
	tracking of controls that may not be applicable	tracking of controls that may not be applicable
11.	The data and information are tightly coupled and it does not provide a means for development, customization and reusing of template for the different types of information systems	The data and information are loosely coupled which allows for the development of templates that can be customized & reused for the security assessment of different information systems
12.	There are higher costs when performing security assessments due to the duplication of efforts	This is limited or no task duplication costs when performing security assessment
13.	It does not provide a fully-integrated approach to security assessment	It provides a fully-integrated approach to security assessment
14.	Tracking of the security assessment to the corrective action plan can be tedious and fraught with errors	The security assessment process drives the corrective action plan
15.	It does not incorporate artificial intelligence in the identification and selection of controls that should be assess for different information system	It provides a basis for the development of artificial intelligence systems that can assist in the identification and selection of the controls that apply for different information systems
16.	It is not in a format that is readily available to support Business Performance Measure Scorecard or Dashboards for assessing and highlighting the security posture of information systems	It provides the basis for the development of a Business Performance Measures Scorecard and Dashboard for assessing and highlighting the security posture of information systems
17.	It establishes interconnections between systems is a manual ad hoc process that is prone to errors and omissions	It provides a more comprehensive integrated approach to establish and track the interconnections between systems and consequently ensure the proper security categorization of the systems
18.	There is no method in place to effectively track the responsibility and authority for management of the different security controls within organization	It provides a method to effectively track responsibility and authority for the different security controls that affect a systems within an organization
19.	It does not provide a fully integrated inventory tracking and mapping for the information systems	It provides a fully integrated inventory tracking and mapping for the information systems
20.	It has the ability to track and manage risks posed to the information system may be limited by human ability to understand their multiple complex systems and their corresponding interactions and interconnections	It enhances the limits of human capability to track, understand and manage risks posed to multiple complex information systems and their interactions and interconnections
21.	Its mapping of the security controls to other standards is a manual and labor-intensive process	Its mapping of the security controls to other standards is pre-programmed in the systems

Table C63 Hypothesis Test of e-Government Relational Technical Controls

Hypothesis Test Summary

	Null Hypothesis	Test	Sig.	Decision
1	The categories of Recode of UseruniqueID to agree and disagree. occur with the specified probabilities.	One-Sample Chi-Square Test	.	Unable to compute.
2	The categories of Recode of UserSingle to agree and disagree. occur with equal probabilities.	One-Sample Chi-Square Test	.011	Reject the null hypothesis.
3	The categories of Recode of ISAMultipleUsers to agree and disagree. occur with the specified probabilities.	One-Sample Chi-Square Test	.	Unable to compute.
4	The categories of Recode of IAnoUses to agree and disagree. occur with equal probabilities.	One-Sample Chi-Square Test	.001	Reject the null hypothesis.
5	The categories of Recode of ASystemUniqueID to agree and disagree. occur with the specified probabilities.	One-Sample Chi-Square Test	.	Unable to compute.
6	The categories of Recode of SystemSingleID to agree and disagree. occur with equal probabilities.	One-Sample Chi-Square Test	.001	Reject the null hypothesis.
7	The categories of Recode of DIAMultipleSystems to agree and disagree. occur with the specified probabilities.	One-Sample Chi-Square Test	.	Unable to compute.

Continued on the next page.

8	The categories of Recode of IAofNOSystems to agree and disagree. occur with equal probabilities.	One-Sample Chi-Square Test	.000	Reject the null hypothesis.
9	The categories of Recode of AuthenticatedIDsmustaccessIS to agree and disagree. occur with equal probabilities.	One-Sample Chi-Square Test	.001	Reject the null hypothesis.
10	The categories of Recode of AuthenticatedIDsmayaccessIS to agree and disagree. occur with equal probabilities.	One-Sample Chi-Square Test	.000	Reject the null hypothesis.
11	The categories of Recode of ACcontrolsanAuthenticatedID to agree and disagree. occur with equal probabilities.	One-Sample Chi-Square Test	.000	Reject the null hypothesis.
12	The categories of Recode of ACmultipleauthenticatedIDs to agree and disagree. occur with the specified probabilities.	One-Sample Chi-Square Test	.	Unable to compute.
13	The categories of Recode of ACcreatesauditrecord to agree and disagree. occur with the specified probabilities.	One-Sample Chi-Square Test	.	Unable to compute.
14	The categories of Recode of ACcreatedmultipleauditrecords to agree and disagree. occur with the specified probabilities.	One-Sample Chi-Square Test	.	Unable to compute.
15	The categories of Recode of AUauditsanAC to agree and disagree. occur with equal probabilities.	One-Sample Chi-Square Test	.000	Reject the null hypothesis.
16	The categories of Recode of AUauditsmultipleAC to agree and disagree. occur with the specified probabilities.	One-Sample Chi-Square Test	.	Unable to compute.
17	The categories of Recode of AUtoSC to agree and disagree. occur with equal probabilities.	One-Sample Chi-Square Test	.000	Reject the null hypothesis.
18	The categories of Recode of AUtoMultipleSC to agree and disagree. occur with equal probabilities.	One-Sample Chi-Square Test	.000	Reject the null hypothesis.
19	The categories of Recode of SCMonitorsanAU to agree and disagree. occur with equal probabilities.	One-Sample Chi-Square Test	.000	Reject the null hypothesis.
20	The categories of Recode of SCmonitormultipleAU to agree and disagree. occur with equal probabilities.	One-Sample Chi-Square Test	.000	Reject the null hypothesis.

Asymptotic significances are displayed. The significance level is .05.

Table C64 Respondent Feedback & Researcher Comments

#	Respondent Feedback	Researcher's Comments
1.	"Users with administrative privileges should have multiple user/process ids: for example, one could be used for performing administrative functions, one for performing non-administrative functions therefore limiting exposure to sensitive assets, one for testing access control for common users, and one for remote login with restricted permissions."	We must first note that addressing the account requirements for systems maintainers is outside the scope of this research. Yet in an attempt to address this comment, the respondents' feedback suggests that the relationship between the user entity and the IA entity should have cardinalities of one and multiple user ids instead of a maximum and minimum of one user id. This is a new school of thought that users should have multiple identifiers so that if a user's password for one system is hacked, the hacker is restricted to a single system associated with that identifier instead of having access to multiple systems. The drawback of this method of assigning multiple identifiers to a user is that they tend to use the same password for the different identifiers or they might choose to write down the multiple identifiers and their corresponding passwords and position it within easy access of computer. This method of implementing multiple identifiers and passwords has the likelihood of creating increased risks to information systems. Typically, there is

#	Respondent Feedback	Researcher's Comments
		heavy administrative overhead involved in supporting this type of configuration. The multiple-identifier/password scenario does not appear to solve the problem associated with having access to multiple information systems. An option may be to assign users a single identifier and multiple tokens (that provide one-time asynchronous passwords) for each system they need to access. This may be a more feasible option from a user and administrative perspective though the costs associated with providing multiple tokens can be substantial.
2.	"Users may have to support multiple roles. These roles may need different user IDs."	See feedback #1.
3.	"I believe unique identification is imperative to the auditing function and (possible) subsequent legal ramifications. If a user is doing something they are not supposed to and are dragged into court, we must be able to prove beyond a shadow of a doubt that individual was the one with the hands on the keyboard. Group accounts make this much more difficult."	Group accounts may be used for granting assess but auditing should be activated at the user level instead of the group level. Auditing at the user level will create extensive audit logs but it will also address the issue of non-repudiation associated with group accounts.

#	Respondent Feedback	Researcher's Comments
4.	"The system/device id should be based on a combination of hardware signatures: for example, for a user's computer workstation on the network, a combination of a MAC address, a motherboard manufacturing batch code, and a hard drive model identification would be sufficient to identify the computer workstation uniquely. Yet, a system/device id is likely to change over time while referring to the same logical unit, such as when upgrading the hard drive of a user's computer workstation: in such cases, multiple system/device ids are necessary; this is where the need for a relational information system arises and provides a better alternative to identify, authenticate, and audit a logical system/device across its different ids over time (i.e. over its lifecycle)."	This comment supports the development of an e-Government Relational Technical Control Model that requires each system/device to have a system/device identifier associated with it. This statement supports the relationship between the system/device and the IA entities.
5.	"Although the possibility of false authentications, I think the likelihood is low is implemented properly, so I think if someone is authenticated, then there is no reason NOT to grant them access."	This statement further supports the relationship between the IA and AC entities.
6.	"For strong and robust IA posture in compliance with most established industry and Federal standards for	This statement appears to support the relationship between the AU and the AC entities for identified and authenticated

#	Respondent Feedback	Researcher's Comments
	C&A, this is a good practice. Usually there will be an audit log or other IA security mechanism that will assist in tracking auditable events?"	entities.
7.	"In today's world, I think it is well accepted that the judicial system has not caught up with cyber crimes. I think proper auditing is a strong step in the right direction to minimizing this gap."	This statement appears to support the relationship between the AU and the AC entities for identified and authenticated entities.

Table C65 Hypothesis Testing for Variables in Section 3 of the Data Collection

Hypothesis Test Summary

	Null Hypothesis	Test	Sig.	Decision
1	The categories defined by Recode of IA2AuthenticatedUsersIDaccessIS to agree and disagree. = 2 and 1 occur with probabilities 0.5 and 0.5.	One-Sample Binomial Test	.000[1]	Reject the null hypothesis.
2	The categories defined by Recode of 55 to agree and disagree. = 2 and 1 occur with probabilities 0.5 and 0.5.	One-Sample Binomial Test	.000[1]	Reject the null hypothesis.
3	The categories defined by Recode of 56 to agree and disagree. = 2 and 1 occur with probabilities 0.5 and 0.5.	One-Sample Binomial Test	.000[1]	Reject the null hypothesis.
4	The categories defined by Recode of 57 to agree and disagree. = 2 and 1 occur with probabilities 0.5 and 0.5.	One-Sample Binomial Test	.000[1]	Reject the null hypothesis.
5	The categories defined by Recode of 60 to agree and disagree. = 2 and 1 occur with probabilities 0.5 and 0.5.	One-Sample Binomial Test	.000[1]	Reject the null hypothesis.
6	The categories defined by Recode of 61 to agree and disagree. = 2 and 1 occur with probabilities 0.5 and 0.5.	One-Sample Binomial Test	.017[1]	Reject the null hypothesis.
7	The categories defined by Recode of 62 to agree and disagree. = 2 and 1 occur with probabilities 0.5 and 0.5.	One-Sample Binomial Test	.001[1]	Reject the null hypothesis.

8	The categories defined by Recode of 66 to agree and disagree. = 2 and 1 occur with probabilities 0.5 and 0.5.	One-Sample Binomial Test	.001[1]	Reject the null hypothesis.
9	The categories defined by Recode of 68 to agree and disagree. = 2 and 1 occur with probabilities 0.5 and 0.5.	One-Sample Binomial Test	.000[1]	Reject the null hypothesis.
10	The categories defined by Recode of 70 to agree and disagree. = 2 and 1 occur with probabilities 0.5 and 0.5.	One-Sample Binomial Test	.000[1]	Reject the null hypothesis.
11	The categories defined by Recode of 72 to agree and disagree. = 2 and 1 occur with probabilities 0.5 and 0.5.	One-Sample Binomial Test	.000[1]	Reject the null hypothesis.
12	The categories defined by Recode of 74 to agree and disagree. = 2 and 1 occur with probabilities 0.5 and 0.5.	One-Sample Binomial Test	.000[1]	Reject the null hypothesis.
13	The categories defined by Recode of 75 to agree and disagree. = 2 and 1 occur with probabilities 0.5 and 0.5.	One-Sample Binomial Test	.001[1]	Reject the null hypothesis.
14	The categories defined by Recode of 76 to agree and disagree. = 2 and 1 occur with probabilities 0.5 and 0.5.	One-Sample Binomial Test	.134[1]	Retain the null hypothesis.
15	The categories defined by Recode of 77 to agree and disagree. = 2 and 1 occur with probabilities 0.5 and 0.5.	One-Sample Binomial Test	.004[1]	Reject the null hypothesis.

16	The categories defined by Recode of 78 to agree and disagree. = 2 and 1 occur with probabilities 0.5 and 0.5.	One-Sample Binomial Test	.000[1]	Reject the null hypothesis.
17	The categories of 79. IA-4: Period of inactivity (days) before disabling a user account occur with equal probabilities.	One-Sample Chi-Square Test	.110	Retain the null hypothesis.
18	The categories of 80. IA-5: Frequence (days) for changing / refreshing authenticators (or passwords) occur with equal probabilities.	One-Sample Chi-Square Test	.001	Reject the null hypothesis.
19	The categories of 81. IA-5: Quantity of user password histories remember and prevent reusing. occur with equal probabilities.	One-Sample Chi-Square Test	.208	Retain the null hypothesis.
20	The categories of 82. IA-5: Minimum number of characters for passwords occur with equal probabilities.	One-Sample Chi-Square Test	.003	Reject the null hypothesis.
21	The categories defined by 83i. Passwords case sensitive = Yes and No occur with probabilities 0.5 and 0.5.	One-Sample Binomial Test	.000[1]	Reject the null hypothesis.
22	The categories defined by 83iii. Using of upper & lower cases = Yes and No occur with probabilities 0.5 and 0.5.	One-Sample Binomial Test	.000[1]	Reject the null hypothesis.
23	The categories defined by 83v. Using special characters = Yes and No occur with probabilities 0.5 and 0.5.	One-Sample Binomial Test	.000[1]	Reject the null hypothesis.
24	The categories defined by 83vi. Minimum requirement for each item = No and Yes occur with probabilities 0.5 and 0.5.	One-Sample Binomial Test	.134[1]	Retain the null hypothesis.
25	The categories defined by Recode of 85 to agree and disagree. = 2 and 1 occur with probabilities 0.5 and 0.5.	One-Sample Binomial Test	.000[1]	Reject the null hypothesis.
26	The categories defined by Recode of 87 to agree and disagree. = 2 and 1 occur with probabilities 0.5 and 0.5.	One-Sample Binomial Test	.000[1]	Reject the null hypothesis.

Asymptotic significances are displayed. The significance level is .05.

[1]Exact significance is displayed for this test.

Table C66 IA Respondent Feedback and Research's Comments

#	Respondent Feedback	Researcher's Comments
1.	"These items (MAC address or IP address) do not directly enhance the security of an information system. It is merely a means to categorize and identify IT assets. It does help in identifying systems that are potentially insecure or could have a high risk value within the information system."	The research agrees with these comments and recommends that devices and systems be identified using identifiers that are specific to them and cannot be easily spoofed by a hacker.
2.	"While helpful, I do not believe that MAC and IP can be relied on for security, but they can indeed improve security posture if used in conjunction with other measures."	See Comment (1).
3.	"Adequate protection must be provided for the use of IP addresses to well-known attacks to prevent rogue devices/systems from acquiring system access and thereby causing widespread damage, data and system compromise."	See Comment (1).
4.	"use of MAC addresses might not be the best solution in a virtual environment"	See Comment (1).
5.	"This is a tough one for me. Because MAC addresses can be spoofed (SANS has demonstrated this attack method in their Ethical Hacking course) they may serve to increase availability, but not confidentiality or integrity. However, an	See Comment (1).

#	Respondent Feedback	Researcher's Comments
	attacker spoofing a MAC address must first be able to identify an internal MAC address to be able to pull this off. That is very difficult and not a preferred method of attack (however it has been done successfully by some very good hackers)"	
6.	"IP's are easily spoofed and in systems that have relied on authenticating IP's those systems are more vulnerable to attacks."	See Comment (1).
7.	"I understand that using the same name gives away the user's login ID, but that could be guessed at most places anyways since there are only a few 'standards' across the industry."	The issue of unique identifiers is being raised from a different perspective indicating that using multiple identifiers does not make a system any more secure as the identifiers can be guessed.
8.	"I disagree with this statement because single sign on is just a way to reduce the complexity of a user to login into multiple systems. I do not believe it increases security. Helps in the administration of identification and authentication."	The researcher agrees with this comment, which failed to reject the null hypothesis.
9.	"Single sign-on does not increase security posture unless it is perhaps reducing the occurrence of passwords being written down and poorly secured."	See comment (8)
10.	"According to Shon Harris, for Single Sign On (SSO) technologies, once a user is in, he is in. If an attacker is able to	See comment (8)

#	Respondent Feedback	Researcher's Comments
	uncover one set of credentials, he shall have access to every resource within the environment that the compromised account has access to."	
11.	"Single sign on has the risk where a compromised password would have access to multiple systems when it is used to log on."	See comment (8)
12.	"Users should use passphrases instead of passwords. It is getting too easy to crack the typical 8 character password."	The research results indicated that at 95 percent significance, the use of password with eight to ten characters coupled with other password characteristics improved the security posture of information systems. In addition, scientific research indicates that breaking passwords composed of eight to ten characters comprised of numbers, upper and lower cases and special characters can take a long time to hack.
13.	"Requiring the use of different unique identifiers for each different information system is • Counterintuitive to good security practice. In my experience, users in such an environment strongly tend to write down their unique user ID's and	This good practice is supported by this research.

#	Respondent Feedback	Researcher's Comments
	passwords and put that piece of paper in, on, or around their desk. Have one identifier but require multiple authenticators instead."	

Table C67 User/Process Entity and IA Risk Management Strategies Association & Correlations

Item	Question	27. Each Users/Processes should have a unique identifier for authentication to an information system.	28. Users/Processes should be restricted to a single user/process id.	29. An IA entity should be capable of identification and authentication of multiple users/processes.	30. An IA entity can exist that does not identify and authenticate users/process. (They may identify and authenticate only systems/devices)
52	**IA-2: Authenticated user/process IDs should be granted access to the information system.**	Somers'd = 0.495 Approx. Sig. = .004 Gamma = 1.000 Approx. Sig. = .004 Spearman rho = .515 Approx. Sig = .014	Somers'd = .552 Approx. Sig. = .002 Gamma = .782 Approx. Sig. = .002 Spearman rho = .582 Approx. Sig = .005	No significant association or correlations	Somers'd = .434 Approx. Sig. = .033 Gamma = .651 Approx. Sig. = .033 Spearman rho = .468 Approx. Sig = .028
53	**IA-2: The identification and authentication control family should be used to manage identifier generator for an information system.**	No significant association or correlations	No significant association or correlations	Somers'd = .500 Approx. Sig. = .005 Gamma = .853 Approx. Sig. = .005 Spearman rho = .500 Approx. Sig = .018	No significant association or correlations

Item	Question	27. Each Users/Processes should have a unique identifier for authentication to an information system.	28. Users/Processes should be restricted to a single user/process id.	29. An IA entity should be capable of identification and authentication of multiple users/processes.	30. An IA entity can exist that does not identify and authenticate users/process. (They may identify and authenticate only systems/devices)
54	**IA-2: The identifier management and the access control entities should be integrated for managing access to applications (residing on the information system) and the information system.**	No significant association or correlations	No significant association or correlations	Somers'd = .548 Approx. Sig. = .002 Gamma = .846 Approx. Sig. = .002 Spearman rho = .548 Approx. Sig = .008	No significant association or correlations
55	**IA-2: The use of multi-factor authentication increases the security posture of information systems.**	Somers'd = .607 Approx. Sig. = .001 Gamma = 1.000 Approx. Sig. = .001 Spearman rho = .633 Approx. Sig = .002	Somers'd = .483 Approx. Sig. = .008 Gamma = .683 Approx. Sig. = .008 Spearman rho = .506 Approx. Sig = .016	No significant association or correlations	No significant association or correlations

Item	Question	27. Each Users/Processes should have a unique identifier for authentication to an information system.	28. Users/Processes should be restricted to a single user/process id.	29. An IA entity should be capable of identification and authentication of multiple users/processes.	30. An IA entity can exist that does not identify and authenticate users/process. (They may identify and authenticate only systems/devices)
56	**IA-2: Identifier generators should be capable of multi-factor authentication.**	No significant association or correlations	No significant association or correlations	Somers'd = .382 Approx. Sig. = .056 Gamma = .600 Approx. Sig. = .056 Spearman rho = .390 Approx. Sig = .072	No significant association or correlations
57	**IA-2: Having one of the factors of multi-factor authentication provided by a device separate from the information system being access, improves the security posture of the information system.**	Somers'd = .607 Approx. Sig. = .001 Gamma = 1.000 Approx. Sig. = .001 Spearman rho = .633 Approx. Sig = .002	No significant association or correlations	No significant association or correlations	No significant association or correlations

Item	Question	27. Each Users/Processes should have a unique identifier for authentication to an information system.	28. Users/Processes should be restricted to a single user/process id.	29. An IA entity should be capable of identification and authentication of multiple users/processes.	30. An IA entity can exist that does not identify and authenticate users/process. (They may identify and authenticate only systems/devices)
58	**IA-2: The use of time synchronous or challenge-response one-time authenticators improves the security posture of information systems.**	Somers'd = .488 Approx. Sig. = .004 Gamma = 1 Approx. Sig. = .004 Spearman rho = .495 Approx. Sig = .019	Somers'd = .383 Approx. Sig. = .051 Gamma = .570 Approx. Sig. = .051 Spearman rho = .408 Approx. Sig = .059	No significant association or correlations	No significant association or correlations
60	**IA-3: System/device ids that should be centrally managed by an information system.**	No significant association or correlations	No significant association or correlations	No significant association or correlations	No significant association or correlations
61	**IA-3: The use of MAC addresses for the identification and authentication of devices/systems improves the security posture of an information system.**	No significant association or correlations	Somers'd = .695 Approx. Sig. = .000 Gamma = .930 Approx. Sig. = .000 Spearman rho = .746 Approx. Sig = .000	No significant association or correlations	No significant association or correlations

Item	Question	27. Each Users/Processes should have a unique identifier for authentication to an information system.	28. Users/Processes should be restricted to a single user/process id.	29. An IA entity should be capable of identification and authentication of multiple users/processes.	30. An IA entity can exist that does not identify and authenticate users/process. (They may identify and authenticate only systems/devices)
62	**IA-3: The use of IP addresses for identification and authentication of devices/systems improves the security posture of an information system.**	No significant association or correlations	Somers'd = .422 Approx. Sig. = .021 Gamma = .633 Approx. Sig. = .021 Spearman rho = .459 Approx. Sig = .031	Somers'd = .459 Approx. Sig. = .004 Gamma = .808 Approx. Sig. =.004 Spearman rho = .482 Approx. Sig = .023	No significant association or correlations
63	**IA-3: The use of bidirectional authentication between devices improves the security posture of an information system.**	No significant association or correlations	No significant association or correlations	Somers'd = .650 Approx. Sig. = .000 Gamma = .929 Approx. Sig. =.000 Spearman rho = .650 Approx. Sig = .001	No significant association or correlations

Item	Question	27. Each Users/Processes should have a unique identifier for authentication to an information system.	28. Users/Processes should be restricted to a single user/process id.	29. An IA entity should be capable of identification and authentication of multiple users/processes.	30. An IA entity can exist that does not identify and authenticate users/process. (They may identify and authenticate only systems/devices)
65	**IA-4: Users, processes, systems and devices must be uniquely identified to an information system.**	No significant association or correlations	Somers'd = .412 Approx. Sig. = .012 Gamma = .643 Approx. Sig. = .012 Spearman rho = .444 Approx. Sig = .038	Somers'd = .551 Approx. Sig. = .003 Gamma = .886 Approx. Sig. = .003 Spearman rho = .552 Approx. Sig = .008	No significant association or correlations
66	**IA-4: Preventing the reuse of user, process, system or device identifiers increases the security posture of an information system.**	No significant association or correlations	Somers'd = .510 Approx. Sig. = .004 Gamma = .720 Approx. Sig. =.004 Spearman rho = .540 Approx. Sig = .010	No significant association or correlations	No significant association or correlations

Item	Question	27. Each Users/Processes should have a unique identifier for authentication to an information system.	28. Users/Processes should be restricted to a single user/process id.	29. An IA entity should be capable of identification and authentication of multiple users/processes.	30. An IA entity can exist that does not identify and authenticate users/process. (They may identify and authenticate only systems/devices)
67	**IA-4: Disabling user identifier after an organization-defined period of inactivity improves the security posture of an information system.**	No significant association or correlations	Somers'd = .387 Approx. Sig. = .031 Gamma = .639 Approx. Sig. =.031 Spearman rho = .413 Approx. Sig = .056	No significant association or correlations	No significant association or correlations
68	**IA-4: The use of user identifiers that do not match the email address of users improves the security posture of an information system.**	No significant association or correlations	Somers'd = .464 Approx. Sig. = .011 Gamma = .680 Approx. Sig. = .011 Spearman rho = .495 Approx. Sig = .019	No significant association or correlations	No significant association or correlations

Item	Question	27. Each Users/Processes should have a unique identifier for authentication to an information system.	28. Users/Processes should be restricted to a single user/process id.	29. An IA entity should be capable of identification and authentication of multiple users/processes.	30. An IA entity can exist that does not identify and authenticate users/process. (They may identify and authenticate only systems/devices)
70	**IA-5: Limiting the reuse of authenticators for users/processes improves the security posture of information systems**	No significant association or correlations	No significant association or correlations	Somers'd = .462 Approx. Sig. = .018 Gamma = .674 Approx. Sig. = .018 Spearman rho = .472 Approx. Sig = .027	No significant association or correlations
71	**IA-5: Limiting the reuse of authenticators for systems/devices improves the security posture of information systems**	No significant association or correlations	Somers'd = .511 Approx. Sig. = .003 Gamma = .761 Approx. Sig. =.003 Spearman rho = .546 Approx. Sig = .009	Somers'd = .388 Approx. Sig. = .045 Gamma = .697 Approx. Sig. = .045 Spearman rho = .388 Approx. Sig = .074	Somers'd = .472 Approx. Sig. = .027 Gamma = .690 Approx. Sig. =.027 Spearman rho = .494 Approx. Sig = .019

Item	Question	27. Each Users/Processes should have a unique identifier for authentication to an information system.	28. Users/Processes should be restricted to a single user/process id.	29. An IA entity should be capable of identification and authentication of multiple users/processes.	30. An IA entity can exist that does not identify and authenticate users/process. (They may identify and authenticate only systems/devices)
72	**IA-5: Establishing the minimum period before requiring a password change improves the security posture of information systems.**	No significant association or correlations	No significant association or correlations	Somers'd = .343 Approx. Sig. = .070 Gamma = .636 Approx. Sig. =.070 Spearman rho = .350 Approx. Sig = .111	No significant association or correlations
73	**IA-5: Establishing the maximum period before requiring a password change improves the security posture of information systems.**	No significant association or correlations	Somers'd = .383 Approx. Sig. = 051 Gamma = .570 Approx. Sig. =.051 Spearman rho = .408 Approx. Sig = .059	No significant association or correlations	No significant association or correlations

Item	Question	27. Each Users/Processes should have a unique identifier for authentication to an information system.	28. Users/Processes should be restricted to a single user/process id.	29. An IA entity should be capable of identification and authentication of multiple users/processes.	30. An IA entity can exist that does not identify and authenticate users/process. (They may identify and authenticate only systems/devices)
74	**IA-5: The use of automated tools to determine the strength of authenticators to resist attacks improves the security posture of an information system.**	Somers'd = .457 Approx. Sig. = .035 Gamma = .828 Approx. Sig. = .035 Spearman rho = .475 Approx. Sig = .026	Somers'd = .454 Approx. Sig. = .012 Gamma = .681 Approx. Sig. = .012 Spearman rho = .479 Approx. Sig = .024	Somers'd = .465 Approx. Sig. = .019 Gamma = .687 Approx. Sig. =.019 Spearman rho = .474 Approx. Sig = .026	No significant association or correlations
75	**IA-5: The use of different unique authenticators (or passwords) for different information systems improves the security posture of the organization.**	No significant association or correlations	Somers'd = .579 Approx. Sig. = .001 Gamma = .772 Approx. Sig. = .001 Spearman rho = .611 Approx. Sig = .003	No significant association or correlations	No significant association or correlations

Item	Question	27. Each Users/Processes should have a unique identifier for authentication to an information system.	28. Users/Processes should be restricted to a single user/process id.	29. An IA entity should be capable of identification and authentication of multiple users/processes.	30. An IA entity can exist that does not identify and authenticate users/process. (They may identify and authenticate only systems/devices)
76	**IA-5: Employing the use of single sign-on improves the security posture of information systems.**	No significant association or correlations	No significant association or correlations	Somers'd = .363 Approx. Sig. = .045 Gamma = .560 Approx. Sig. =.045 Spearman rho = .389 Approx. Sig = .074	No significant association or correlations
77	**IA-5: Using one-time passwords improves the security posture of information systems.**	No significant association or correlations	No significant association or correlations	Somers'd = .338 Approx. Sig. = .063 Gamma = .575 Approx. Sig. =.063 Spearman rho = .358 Approx. Sig = .102	No significant association or correlations

Item	Question	27. Each Users/Processes should have a unique identifier for authentication to an information system.	28. Users/Processes should be restricted to a single user/process id.	29. An IA entity should be capable of identification and authentication of multiple users/processes.	30. An IA entity can exist that does not identify and authenticate users/process. (They may identify and authenticate only systems/devices)
78	**IA-5: Restricting the number of accounts individuals have on multiple information systems improves their security posture.**	No significant association or correlations	No significant association or correlations	Somers'd = .422 Approx. Sig. = .022 Gamma = .675 Approx. Sig. = .022 Spearman rho = .437 Approx. Sig = .042	No significant association or correlations
79	**IA-4: What should be the period of inactivity before a user account is disabled?**	No significant association or correlations	No significant association or correlations	No significant association or correlations	No significant association or correlations
80	**IA-5: How often should authenticators (or passwords) be changed/refreshed?**	Somers'd = -.253 Approx. Sig. = .066 Gamma = -.600 Approx. Sig. = .066 Spearman rho = -.282 Approx. Sig = .203	No significant association or correlations	No significant association or correlations	No significant association or correlations

Item	Question	27. Each Users/Processes should have a unique identifier for authentication to an information system.	28. Users/Processes should be restricted to a single user/process id.	29. An IA entity should be capable of identification and authentication of multiple users/processes.	30. An IA entity can exist that does not identify and authenticate users/process. (They may identify and authenticate only systems/devices)
81	**IA-5: How many password histories should an information system remember and prevent users from reusing?**	No significant association or correlations	Somers'd = .331 Approx. Sig. = .036 Gamma = .474 Approx. Sig. =.036 Spearman rho = .391 Approx. Sig = .072	No significant association or correlations	No significant association or correlations
82	**IA-5: What should be the minimum number of characters required for passwords?**	No significant association or correlations	No significant association or correlations	Somers'd = -.380 Approx. Sig. = .023 Gamma = -.676 Approx. Sig. = .023 Spearman rho = -.406 Approx. Sig = .061	No significant association or correlations
83i	**Requiring passwords to be case sensitive**	No significant association or correlations	No significant association or correlations	No significant association or correlations	No significant association or correlations

Item	Question	27. Each Users/Processes should have a unique identifier for authentication to an information system.	28. Users/Processes should be restricted to a single user/process id.	29. An IA entity should be capable of identification and authentication of multiple users/processes.	30. An IA entity can exist that does not identify and authenticate users/process. (They may identify and authenticate only systems/devices)
83ii	**Requiring that the password exceeds a certain number of characters**	This value is a constant	This value is a constant	This value is a constant	This value is a constant
83iii	**Requiring the use of both upper and lower case letters**	No significant association or correlations	No significant association or correlations	No significant association or correlations	No significant association or correlations
83iv	**Requiring the use of numbers**	This value is a constant	This value is a constant	This value is a constant	This value is a constant
83v	**Requiring the use of special characters**	No significant association or correlations	No significant association or correlations	No significant association or correlations	No significant association or correlations
83vi	**Having a minimum requirement for each of the items listed above**	No significant association or correlations	No significant association or correlations	No significant association or correlations	No significant association or correlations

Item	Question	27. Each Users/Processes should have a unique identifier for authentication to an information system.	28. Users/Processes should be restricted to a single user/process id.	29. An IA entity should be capable of identification and authentication of multiple users/processes.	30. An IA entity can exist that does not identify and authenticate users/process. (They may identify and authenticate only systems/devices)
85	**IA-6: Obscuring of feedback during authentication improves the security posture of information systems.**	No significant association or correlations	Somers'd = .361 Approx. Sig. = .048 Gamma = .531 Approx. Sig. =.048 Spearman rho = .396 Approx. Sig = .068	Somers'd = .478 Approx. Sig. = .006 Gamma = .789 Approx. Sig. =.006 Spearman rho = .488 Approx. Sig = .021	Somers'd = .415 Approx. Sig. = .027 Gamma = .659 Approx. Sig. =.027 Spearman rho = .448 Approx. Sig = .037
86	**IA-7: The use of cryptographic modules during authentication improves the security posture of information systems.**	No significant association or correlations	No significant association or correlations	No significant association or correlations	Somers'd = .398 Approx. Sig. = .014 Gamma = .750 Approx. Sig. =.014 Spearman rho = .418 Approx. Sig = .053

Item	Question	27. Each Users/Processes should have a unique identifier for authentication to an information system.	28. Users/Processes should be restricted to a single user/process id.	29. An IA entity should be capable of identification and authentication of multiple users/processes.	30. An IA entity can exist that does not identify and authenticate users/process. (They may identify and authenticate only systems/devices)
87	**IA-8: The identification and authentication of non-organizational users improves the security posture of the information system.**	No significant association or correlations	Somers'd = .397 Approx. Sig. = .019 Gamma = .622 Approx. Sig. =.019 Spearman rho = .438 Approx. Sig = .042	No significant association or correlations	No significant association or correlations

Table C68 System/Device Entity and IA Risk Management Strategies Association & Correlations

Item	Question	32. A System / Device should have a unique identifier for authentication to an information system.	33. A System / Device should be restricted to a single system / device id.	34. An IA entity should be capable of identification and authentication of multiple systems / devices.	35. An IA entity can exist that does not identify and authenticate systems/devices (They may identify and authenticate only Users/Processes)
52	IA-2: Authenticated user / process IDs should be granted access to the information system.	Somers'd = .520 Approx. Sig. = .002 Gamma = .865 Approx. Sig. =.002 Spearman rho = .532 Approx. Sig = .011	Somers'd = .652 Approx. Sig. = .000 Gamma = .936 Approx. Sig. =.000 Spearman rho = .676 Approx. Sig = .001	Somers'd = .410 Approx. Sig. = .025 Gamma = .718 Approx. Sig. =.025 Spearman rho = .418 Approx. Sig = .053	No significant association or correlations

Item	Question	32. A System / Device should have a unique identifier for authentication to an information system.	33. A System / Device should be restricted to a single system / device id.	34. An IA entity should be capable of identification and authentication of multiple systems / devices.	35. An IA entity can exist that does not identify and authenticate systems/devices (They may identify and authenticate only Users/Processes)
53	IA-2: The identification and authentication control family should be use to manage identifier generator for an information system.	Somers'd = .437 Approx. Sig. = .016 Gamma = .806 Approx. Sig. = .016 Spearman rho = .437 Approx. Sig = .042	Somers'd = .648 Approx. Sig. = .000 Gamma = .953 Approx. Sig. =.000 Spearman rho = .681 Approx. Sig = .000	Somers'd = .690 Approx. Sig. = .000 Gamma = 1.00 Approx. Sig. =.000 Spearman rho = .690 Approx. Sig = .000	Somers'd = .829 Approx. Sig. = .000 Gamma = 1.000 Approx. Sig. = .000 Spearman rho = .862 Approx. Sig = .000

Item	Question	32. A System / Device should have a unique identifier for authentication to an information system.	33. A System / Device should be restricted to a single system / device id.	34. An IA entity should be capable of identification and authentication of multiple systems / devices.	35. An IA entity can exist that does not identify and authenticate systems/devices (They may identify and authenticate only Users/Processes)
54	**IA-2: The identifier management and the access control entities should be integrated for managing access to applications (residing on the information system) and the information system.**	No significant association or correlations	Somers'd = .420 Approx. Sig. = .020 Gamma = .679 Approx. Sig. =.020 Spearman rho = .439 Approx. Sig = .041	Somers'd = .548 Approx. Sig. = .002 Gamma = .846 Approx. Sig. =.002 Spearman rho = .548 Approx. Sig = .008	Somers'd = .792 Approx. Sig. = .000 Gamma = 1.000 Approx. Sig. = .000 Spearman rho = .821 Approx. Sig = .000

Item	Question	32. A System / Device should have a unique identifier for authentication to an information system.	33. A System / Device should be restricted to a single system / device id.	34. An IA entity should be capable of identification and authentication of multiple systems / devices.	35. An IA entity can exist that does not identify and authenticate systems/devices (They may identify and authenticate only Users/Processes)
55	**IA-2: The use of multi-factor authentication increases the security posture of information systems.**	No significant association or correlations	Somers'd = .437 Approx. Sig. = .024 Gamma = .694 Approx. Sig. =.024 Spearman rho = .452 Approx. Sig = .035	Somers'd = .458 Approx. Sig. = .012 Gamma = .760 Approx. Sig. =.012 Spearman rho = .467 Approx. Sig = .028	No significant association or correlations
56	**IA-2: Identifier generators should be capable of multi-factor authentication.**	Somers'd = .411Approx. Sig. = .026Gamma = .718Approx. Sig. =.026 Spearman	Somers'd = .610Approx. Sig. = .000Gamma = .912Approx. Sig. = .000 Spearman rho	Somers'd = .654Approx. Sig. = .000Gamma = .931Approx. Sig. =.000 Spearman rho =	No significant association or correlations

Item	Question	32. A System / Device should have a unique identifier for authentication to an information system.	33. A System / Device should be restricted to a single system / device id.	34. An IA entity should be capable of identification and authentication of multiple systems / devices.	35. An IA entity can exist that does not identify and authenticate systems/devices (They may identify and authenticate only Users/Processes)
		rho = .420Approx. Sig = .052	= .634Approx. Sig = .002	.659Approx. Sig = .001	
57	IA-2: Having one of the factors of multi-factor authentication provided by a device separate from the information system being access, improves the security posture of the information system.	Somers'd = .545 Approx. Sig. = .002 Gamma = .848 Approx. Sig. =.002 Spearman rho = .556 Approx. Sig = .007	Somers'd = .437 Approx. Sig. = .024 Gamma = .694 Approx. Sig. =.024 Spearman rho = .452 Approx. Sig = .035	Somers'd = .458 Approx. Sig. = .012 Gamma = .760 Approx. Sig. =.012 Spearman rho = .467 Approx. Sig = .028	No significant association or correlations

Item	Question	32. A System / Device should have a unique identifier for authentication to an information system.	33. A System / Device should be restricted to a single system / device id.	34. An IA entity should be capable of identification and authentication of multiple systems / devices.	35. An IA entity can exist that does not identify and authenticate systems/devices (They may identify and authenticate only Users/Processes)
58	**IA-2: The use of time synchronous or challenge-response one-time authenticators improves the security posture of information systems.**	Somers'd = .574 Approx. Sig. = .001 Gamma = .895 Approx. Sig. =.001 Spearman rho = .574 Approx. Sig = .005	Somers'd = .452 Approx. Sig. = .016 Gamma = .694 Approx. Sig. =.016 Spearman rho = .473 Approx. Sig = .026	Somers'd = .467 Approx. Sig. = .012 Gamma = .778 Approx. Sig. =.012 Spearman rho = .467 Approx. Sig = .029	No significant association or correlations
60	**IA-3: System / device ids that should be centrally manage by an information system.**	No significant association or correlations	Somers'd = .436 Approx. Sig. = .014 Gamma = .642 Approx. Sig. =.025 Spearman rho =	No significant association or correlations	Somers'd = .770 Approx. Sig. = .000 Gamma = .964 Approx. Sig. =.000 Spearman rho =

Item	Question	32. A System / Device should have a unique identifier for authentication to an information system.	33. A System / Device should be restricted to a single system / device id.	34. An IA entity should be capable of identification and authentication of multiple systems / devices.	35. An IA entity can exist that does not identify and authenticate systems/devices (They may identify and authenticate only Users/Processes)
			.478 Approx. Sig = .025		.801 Approx. Sig = .000
61	IA-3: The use of MAC addresses for the identification and authentication of devices / systems improves the security posture of an information system.	No significant association or correlations	Somers'd = .459 Approx. Sig. = .016 Gamma = .650 Approx. Sig. =.016 Spearman rho = .501 Approx. Sig = .018	No significant association or correlations	No significant association or correlations

Item	Question	32. A System / Device should have a unique identifier for authentication to an information system.	33. A System / Device should be restricted to a single system / device id.	34. An IA entity should be capable of identification and authentication of multiple systems / devices.	35. An IA entity can exist that does not identify and authenticate systems/devices (They may identify and authenticate only Users/Processes)
62	**IA-3: The use of IP addresses for identification and authentication of devices / systems improves the security posture of an information system.**	No significant association or correlations	No significant association or correlations	No significant association or correlations	No significant association or correlations
63	**IA-3: The use of bidirectional authentication between devices improves the security posture of an information system.**	Somers'd = .388 Approx. Sig. = .045 Gamma = .697 Approx. Sig. =.045 Spearman rho = .388	No significant association or correlations	Somers'd = .476 Approx. Sig. = .012 Gamma = .778 Approx. Sig. =.012 Spearman rho = .467 Approx. Sig = .029	Somers'd = .440 Approx. Sig. = .026 Gamma = .655 Approx. Sig. =.026 Spearman rho = .456

Item	Question	32. A System / Device should have a unique identifier for authentication to an information system.	33. A System / Device should be restricted to a single system / device id.	34. An IA entity should be capable of identification and authentication of multiple systems / devices.	35. An IA entity can exist that does not identify and authenticate systems/devices (They may identify and authenticate only Users/Processes)
		Approx. Sig = .074			Approx. Sig = .033
65	**IA-4: Users, processes, systems and devices must be uniquely identified to an information system.**	Somers'd = .423 Approx. Sig. = .041 Gamma = .746 Approx. Sig. =.041 Spearman rho = .424 Approx. Sig = .049	No significant association or correlations	Somers'd = .551 Approx. Sig. = .003 Gamma = .886 Approx. Sig. =.003 Spearman rho = .552 Approx. Sig = .008	No significant association or correlations

Item	Question	32. A System / Device should have a unique identifier for authentication to an information system.	33. A System / Device should be restricted to a single system / device id.	34. An IA entity should be capable of identification and authentication of multiple systems / devices.	35. An IA entity can exist that does not identify and authenticate systems/devices (They may identify and authenticate only Users/Processes)
66	**IA-4: Preventing the reuse of user, process, system or device identifiers increases the security posture of an information system.**	No significant association or correlations	Somers'd = .420 Approx. Sig. = .031 Gamma = .625 Approx. Sig. =.031 Spearman rho = .447 Approx. Sig = .037	No significant association or correlations	Somers'd = .465 Approx. Sig. = .016 Gamma = .673 Approx. Sig. =.016 Spearman rho = .488 Approx. Sig = .021
67	**IA-4: Disabling user identifier after an organization-defined period of inactivity improves the security**	No significant association or correlations	Somers'd = .488 Approx. Sig. = .014 Gamma = .708 Approx. Sig. =.014 Spearman rho =	Somers'd = .388 Approx. Sig. = .045 Gamma = .697 Approx. Sig. =.045 Spearman rho = .388	Somers'd = .602 Approx. Sig. = .000 Gamma = .906 Approx. Sig. =.000 Spearman rho =

Item	Question	32. A System / Device should have a unique identifier for authentication to an information system.	33. A System / Device should be restricted to a single system / device id.	34. An IA entity should be capable of identification and authentication of multiple systems / devices.	35. An IA entity can exist that does not identify and authenticate systems/devices (They may identify and authenticate only Users/Processes)
	posture of an information system.		.512 Approx. Sig = .015	Approx. Sig = .074	.624 Approx. Sig = .002
68	**IA-4: The use of user identifiers that do not match the email address of users improves the security posture of an information system.**	No significant association or correlations	Somers'd = .433Approx. Sig. = .036Gamma = .638Approx. Sig. =.036 Spearman rho = .454Approx. Sig = .034	Somers'd = .422Approx. Sig. = .022Gamma = .675Approx. Sig. =.022 Spearman rho = .437Approx. Sig = .042	Somers'd = .393Approx. Sig. = .034Gamma = .600Approx. Sig. =.034 Spearman rho = .423Approx. Sig = .050

Item	Question	32. A System / Device should have a unique identifier for authentication to an information system.	33. A System / Device should be restricted to a single system / device id.	34. An IA entity should be capable of identification and authentication of multiple systems / devices.	35. An IA entity can exist that does not identify and authenticate systems/devices (They may identify and authenticate only Users/Processes)
70	IA-5: Limiting the reuse of authenticators for users / processes improves the security posture of information systems	Somers'd = .476 Approx. Sig. = .008 Gamma = .787 Approx. Sig. =.008 Spearman rho = .486 Approx. Sig = .022	Somers'd = .471 Approx. Sig. = .016 Gamma = .711 Approx. Sig. =.016 Spearman rho = .485 Approx. Sig = .022	Somers'd = .717 Approx. Sig. = .000 Gamma = .957 Approx. Sig. =.000 Spearman rho = .732 Approx. Sig = .000	Somers'd = .444 Approx. Sig. = .036 Gamma = .577 Approx. Sig. =.036 Spearman rho = .471 Approx. Sig = .027
71	IA-5: Limiting the reuse of authenticators for systems / devices improves the security posture of information systems	No significant association or correlations	Somers'd = .488 Approx. Sig. = .014 Gamma = .708 Approx. Sig. =.014 Spearman rho =	Somers'd = .574 Approx. Sig. = .001 Gamma = .895 Approx. Sig. =.001 Spearman rho = .574	Somers'd = .602 Approx. Sig. = .000 Gamma = .906 Approx. Sig. =.000 Spearman rho =

Item	Question	32. A System / Device should have a unique identifier for authentication to an information system.	33. A System / Device should be restricted to a single system / device id.	34. An IA entity should be capable of identification and authentication of multiple systems / devices.	35. An IA entity can exist that does not identify and authenticate systems/devices (They may identify and authenticate only Users/Processes)
			.512 Approx. Sig = .015	Approx. Sig = .005	.624 Approx. Sig = .002
72	IA-5: Establishing the minimum period before requiring a password change improves the security posture of information systems.	No significant association or correlations	Somers'd = .496 Approx. Sig. = .013 Gamma = .688 Approx. Sig. =.013 Spearman rho = .533 Approx. Sig = .011	Somers'd = .514 Approx. Sig. = .002 Gamma = .863 Approx. Sig. =.002 Spearman rho = .524 Approx. Sig = .012	Somers'd = .636 Approx. Sig. = .000 Gamma = .913 Approx. Sig. =.000 Spearman rho = .677 Approx. Sig = .001

Item	Question	32. A System / Device should have a unique identifier for authentication to an information system.	33. A System / Device should be restricted to a single system / device id.	34. An IA entity should be capable of identification and authentication of multiple systems / devices.	35. An IA entity can exist that does not identify and authenticate systems/devices (They may identify and authenticate only Users/Processes)
73	**IA-5: Establishing the maximum period before requiring a password change improves the security posture of information systems.**	No significant association or correlations	No significant association or correlations	Somers'd = .467 Approx. Sig. = .012 Gamma = .778 Approx. Sig. =.012 Spearman rho = .467 Approx. Sig = .029	Somers'd = .541 Approx. Sig. = .001 Gamma = .854 Approx. Sig. =.001 Spearman rho = .560 Approx. Sig = .007
74	**IA-5: The use of automated tools to determine the strength of authenticators to resist attacks improves the security posture of**	Somers'd = .446Approx. Sig. = .020Gamma = .750Approx. Sig. =.020 Spearman	No significant association or correlations	Somers'd = .539Approx. Sig. = .002Gamma = .846Approx. Sig. =.002 Spearman rho =	No significant association or correlations

Item	Question	32. A System / Device should have a unique identifier for authentication to an information system.	33. A System / Device should be restricted to a single system / device id.	34. An IA entity should be capable of identification and authentication of multiple systems / devices.	35. An IA entity can exist that does not identify and authenticate systems/devices (They may identify and authenticate only Users/Processes)
	information system.	rho = .455Approx. Sig = .033		.549Approx. Sig = .008	
75	**IA-5: The use of different unique authenticators (or passwords) for different information systems improves the security posture of the organization.**	No significant association or correlations	No significant association or correlations	No significant association or correlations	Somers'd = .413 Approx. Sig. = .033 Gamma = .621 Approx. Sig. =.033 Spearman rho = .434 Approx. Sig = .043

Item	Question	32. A System / Device should have a unique identifier for authentication to an information system.	33. A System / Device should be restricted to a single system / device id.	34. An IA entity should be capable of identification and authentication of multiple systems / devices.	35. An IA entity can exist that does not identify and authenticate systems/devices (They may identify and authenticate only Users/Processes)
76	**IA-5: Employing the use of single sign-on improves the security posture of information systems.**	No significant association or correlations	No significant association or correlations	Somers'd = .363 Approx. Sig. = .045 Gamma = .560 Approx. Sig. =.045 Spearman rho = .389 Approx. Sig = .074	No significant association or correlations
77	**IA-5: Using one-time passwords improves the security posture of information systems.**	No significant association or correlations	Somers'd = .403 Approx. Sig. = .001 Gamma = .621 Approx. Sig. = .001 Spearman rho = .463	Somers'd = .471 Approx. Sig. = .004 Gamma = .744 Approx. Sig. =.004 Spearman rho = .498 Approx. Sig = .018	Somers'd = .405 Approx. Sig. = .019 Gamma = .596 Approx. Sig. =.019 Spearman rho = .445

Item	Question	32. A System / Device should have a unique identifier for authentication to an information system.	33. A System / Device should be restricted to a single system / device id.	34. An IA entity should be capable of identification and authentication of multiple systems / devices.	35. An IA entity can exist that does not identify and authenticate systems/devices (They may identify and authenticate only Users/Processes)
			Approx. Sig = .030		Approx. Sig = .038
78	**IA-5: Restricting the number of accounts individuals have on multiple information systems improves their security posture.**	No significant association or correlations	No significant association or correlations	Somers'd = .422 Approx. Sig. = .022 Gamma = .675 Approx. Sig. =.022 Spearman rho = .437 Approx. Sig = .042	Somers'd = .611 Approx. Sig. = .000 Gamma = .875 Approx. Sig. =.000 Spearman rho = .663 Approx. Sig = .001

Item	Question	32. A System / Device should have a unique identifier for authentication to an information system.	33. A System / Device should be restricted to a single system / device id.	34. An IA entity should be capable of identification and authentication of multiple systems / devices.	35. An IA entity can exist that does not identify and authenticate systems/devices (They may identify and authenticate only Users/Processes)
79	IA-4: What should be the period of inactivity before a user account is disabled?	No significant association or correlations	No significant association or correlations	No significant association or correlations	No significant association or correlations
80	IA-5: How often should authenticators (or passwords) be changed / refreshed?	No significant association or correlations	No significant association or correlations	No significant association or correlations	No significant association or correlations
81	IA-5: How many password histories should an information system remember and prevent users from reusing?	No significant association or correlations	No significant association or correlations	No significant association or correlations	No significant association or correlations

Item	Question	32. A System / Device should have a unique identifier for authentication to an information system.	33. A System / Device should be restricted to a single system / device id.	34. An IA entity should be capable of identification and authentication of multiple systems / devices.	35. An IA entity can exist that does not identify and authenticate systems/devices (They may identify and authenticate only Users/Processes)
82	IA-5: What should be the minimum number of characters required for passwords?	No significant association or correlations	No significant association or correlations	No significant association or correlations	No significant association or correlations
83i	Requiring passwords to be case sensitive	No significant association or correlations	No significant association or correlations	No significant association or correlations	No significant association or correlations
83ii	Requiring that the password exceeds a certain number of characters	This value is a constant	This value is a constant	This value is a constant	This value is a constant
83iii	Requiring the use of both upper and lower case	No significant association or	No significant association or	No significant association or	No significant association or

Item	Question	32. A System / Device should have a unique identifier for authentication to an information system.	33. A System / Device should be restricted to a single system / device id.	34. An IA entity should be capable of identification and authentication of multiple systems / devices.	35. An IA entity can exist that does not identify and authenticate systems/devices (They may identify and authenticate only Users/Processes)
	letters	correlations	correlations	correlations	correlations
83iv	**Requiring the use of numbers**	This value is a constant	This value is a constant	This value is a constant	This value is a constant
83v	**Requiring the use of special characters**	No significant association or correlations	No significant association or correlations	No significant association or correlations	No significant association or correlations
83vi	**Having a minimum requirement for each of the items listed above**	No significant association or correlations	No significant association or correlations	No significant association or correlations	No significant association or correlations

Item	Question	32. A System / Device should have a unique identifier for authentication to an information system.	33. A System / Device should be restricted to a single system / device id.	34. An IA entity should be capable of identification and authentication of multiple systems / devices.	35. An IA entity can exist that does not identify and authenticate systems/devices (They may identify and authenticate only Users/Processes)
85	**IA-6: Obscuring of feedback during authentication improves the security posture of information systems.**	Somers'd = .411Approx. Sig. = .026Gamma = .718Approx. Sig. =.026 Spearman rho = .420Approx. Sig = .052	Somers'd = .426Approx. Sig. = .015Gamma = .659Approx. Sig. =.015 Spearman rho = .458Approx. Sig = .032	Somers'd = .645Approx. Sig. = .000Gamma = .931Approx. Sig. =.000 Spearman rho = .659Approx. Sig = .001	Somers'd = .659Approx. Sig. = .000Gamma = .918Approx. Sig. =.000 Spearman rho = .701Approx. Sig = .000
86	**IA-7: The use of cryptographic modules during authentication improves the security posture of information**	No significant association or correlations	Somers'd = .372 Approx. Sig. = .030 Gamma = .627 Approx. Sig. =.030 Spearman rho =	Somers'd = .448 Approx. Sig. = .022 Gamma = .765 Approx. Sig. =.022 Spearman rho = .449	Somers'd = .653 Approx. Sig. = .000 Gamma = 1.000 Approx. Sig. = .000 Spearman rho =

Item	Question	32. A System / Device should have a unique identifier for authentication to an information system.	33. A System / Device should be restricted to a single system / device id.	34. An IA entity should be capable of identification and authentication of multiple systems / devices.	35. An IA entity can exist that does not identify and authenticate systems/devices (They may identify and authenticate only Users/Processes)
	systems.		.390 Approx. Sig = .073	Approx. Sig = .036	.680 Approx. Sig = .001
87	**IA-8: The identification and authentication of non-organizational users improves the security posture of the information system.**	No significant association or correlations	Somers'd = .496 Approx. Sig. = .013 Gamma = .688 Approx. Sig. =.013 Spearman rho = .533 Approx. Sig = .011	Somers'd = .514 Approx. Sig. = .002 Gamma = .863 Approx. Sig. =.002 Spearman rho = .524 Approx. Sig = .012	Somers'd = .636 Approx. Sig. = .000 Gamma = .913 Approx. Sig. =.000 Spearman rho = .677 Approx. Sig = .001

Appendix D: Glossary of Terms

Term	Acronym	Definition
Information Assurance	IA	Information Assurance (IA) is a risk management tool. It is defined by the National Security Agency FAQ #2 as "Information Assurance comprises measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities." Information assurance reduces the probability of security vulnerability and minimizes the effects should a security incident occurs. IA provides the guiding principles and audit to the underlying information security (InfoSec) process across an enterprise. IA affirms the stakeholders' trust, confidence and the quality of information in areas of confidentiality, integrity and availability of information being processed. (Ng R. 2009)
Risk	NA	The probability of failure, harm, loss, damage, injury or other undesirable event occurring
Risk management	NA	Risk management involves identifying, analyzing, mitigating, transferring and managing of risks to an organizationally acceptable level to ensure that we maximize positive events and minimize the consequences of adverse events. A process of using risk assessment to make decision about maintaining a desired level of risk
Taxonomy	NA	The Merriam-Webster online dictionary defines taxonomy as 'the study of the general principles of scientific classification.' The word 'taxonomy' originates from the ancient Greek word taxis-nomos. Taxis mean order or arrangement and nomos means law or science. These two words together in taxonomy provide the meaning of the practice and science of classification. A taxonomy classification

Term	Acronym	Definition
		usually results in a hierarchical structure of classes with supertype – subtype relationships. This super-type – sub-type can be in the form of parent-child hierarchy, an organization of things in the form of an alphabetical list, object-process or other forms.

Bibliography

Abkowitz M. D. (2008) "Operational risk management : a case study approach to effective planning and response" John Wiley & Sons, Inc.

Baskerville, R. (1993) Information systems security design methods: Implications for information systems development. ACM Computing Surveys, 25(4), 375-414

Besner, C., & Hobbs, B. (2006). The perceived value and potential contribution of project management practices to project success. Project Management Journal, 37(3), 12.

Blerkom, M. L. (2009). Measurement and Statistics for Teachers. Routledge, Taylor & Francis Group

Bonham. S. S (2008). Actionable Strategies Through Integrated Performance, Process, Project, and Risk Management. Artech House

Briney A. and Prince F. Does size matter? Information Security, September 2002 36-54

Christmann E. P. and Baggett J. L. (2009) Interpreting Assessment Data – Statistical Techniques You Can Use.

Charette, R. N. (1989). Software Engineering Risk Analysis and Management. New York: McGraw-Hill/Intertext.

D'Arcy J. and Hovav A. (2009) "An Integrative Framework for the Study of Information Security Management Research" Handbook of Research on Information Security and Assurance by Information Science Reference p. 55

Fink A. (2009) "How to Conduct Surveys – A Step-by-Step Guide" 4th Editions Sage Publications Inc.

Frank M. V. (2008) "Choosing safety : a guide to using probabilistic risk assessment and decision analysis in complex, high-consequence systems." Resources for the Future

Gupta J. N.D. and Sharma S. K. (2009) "Handbook of research on information security and assurance" Information Science Reference

Gordon, L.A., & Loeb, M.P. (2002). The economics of information security investment. ACM Transactions on Information and System Security, 5(4), 438-457.

Gravetter F. J. and Wallnau L. B (2002) "Essentials of Statistics for the Behavioral Sciences – Fourth Eidition" Wadsworth Thomson Learning Academic Resource Center

http://en.wikipedia.org/wiki/Taxonomy
http://katrina.house.gov/hearings/12_14_05/witness_list_121405.htm
http://www.ftc.gov/opa/2006/01/choicepoint.shtm
http://www.fsa.gov.uk/pages/Library/Communication/PR/2009/099.shtml
http://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf
http://www.merriam-webster.com/dictionary/taxonomy
http://www.time.com/time/nation/article/0,8599,1098371,00.html
http://www.whitehouse.gov/omb/assets/reports/fy2008_fisma.pdf
Hovav, A. (2005). A framework for the study of cyber-liability. Jeju Island, Korea: KMIS
Jaquith, A. (2007). Security metrics: Replacing fear, uncertainty and doubt. New Jersey: Addison-Wesley.
Keyes J. (2008) Leading IT projects: The IT Manager's Guide
Kaplan, J. (2009) Be Safe Out there p. 18 PMI Network, Vol 23, No.1
Kaplan, R. M., and Saccuzzo, D.P. (1993). Psychological Testing: Principles Applications and Issues (3rd Edition). Brooks/Cole Publishing, Pacific Grove, CA.
Kerzner H. (2006) “Project Management - A Systems Approach to Planning, Scheduling, and Controlling” Ninth Edition. John Wiley & Sons, Inc.
Ladika, S (2009) The Incredible Shrinking Team. PM Network Vol 23, No. 1 p. 40-44
Lester J. D., Lester J. D. Jr (2005) “The Essential Guide – Research Writing Across the Disciplines” Third Edition. Pearson Longman
Ma, Q. & Pearson, J. M. (2005). ISO 17799: Best practices in information security management? Communications of the AIS, 15, 577-591
Macaulay T. (2009) "Critical Infrastructure: Understanding its Components Parts, Vulnerabilities, Operating Risks and Interdependencies" CRC Press
Mantel S. J. et al. “Project Management in Practice Second Edition” John Wiley & Sons, Inc 2005
Ng R. (2009) “A Holistic Approach to Information Security Assurance and Risk Management in an Enterprise” Handbook of Research on Information Security and Assurance by Information Science Reference p. 43

Park J. S. and Land J. K (2009) “E-Commerce: The Benefits, Security Risks, and Countermeasures” Handbook of Research on Information Security and Assurance by Information Science Reference p. 16

Perrow C. (2007) "The next catastrophe : reducing our vulnerabilities to natural, industrial, and terrorist disasters" Princeton University Press

PMI today. A Supplement to PM network (May 2009). Published by the Project Management Institute

Project Management Institute. (2008) A guide to the project management body of knowledge (PMBOK guide) (4th Edition). Newtown Square, PA: Project Management Institute

Jen R. (2009). Visual Ishikawa Risk Techniques (VIRT) – An Approach to Risk Management. PMI Virtual Library

Sarantakos S. (2007) “A Toolkit for Quantitative Data Analysis using SPSS” Palgrave Macmillan

Shore B. (2008). Systematic Biases and Culture in Project Failures. Project Management Journal December 2008, p. 10.

Tan, D. (2002). Quantitative Risk Analysis Step-By-Step. Retrieved from http://www.sans.org/reading_room/whitepapers/auditing/849.php

Tejay, G. (2005). Making sense of information systems security standards. Eleventh Americas Conference on Information Systems. Omaha, NE.

Wheatley M (2009) “An inside Job”. Project Management Network July 2009, Volume 23. No. 7 p. 47.

Whitman, M & Mattord, H. (2005), Principles of information security, second edition. Boston: Course Technology

Whitman, M & Mattord, H (2008), Management of Information Security, second edition. Thomson Course Technology