A Case Study on Effective IS Governance within a Department of Defense Organization

Christopher Furton

Syracuse University

Abstract

This case study develops influencing factor that should be considered when developing an effective information security governance program with a Department of Defense weapons system test and evaluation organization. The influencing factors are then incorporated into an existing governance framework developed by A. Da Veiga and J. H. P. Eloff (2007). The result is a unique framework tailored to the organization which can be used as the foundation to building a holistic information security program.

A Case Study on Effective IS Governance within a Department of Defense Organization

With the advancements of technology and the Internet, security of information has become a substantial concern for many companies, non-profits, government agencies, and educational institutions. With an abundance of information available to help organization's establish information security programs, the challenge still exists on how to structure those programs to maximize benefits and reduce risk. Information Technology (IT) security governance plays a critical role with integration of business models with IT security models. Through the use of an IT security governance framework, organizations can develop appropriate information security components and align them with their overall strategic, business, and technical objectives and goals (Veiga & Eloff, 2007).

The IT Security governance framework, along with the selected information security components, lives within the context of the Information Technology Security Architecture (ITSA) Framework developed by Bernard and Ho (2008). The intent of the IT security governance framework is to further explore the first layer of the ITSA Framework and provide organizations with a launching point in developing their security governance programs. Additionally, an important aspect of the IT security governance framework is that each organization can develop a unique framework that fits their needs.

This case study paper will further explore IT security governance frameworks by assessing influencing factors that must be considered and developing a unique framework applicable to a Department of Defense weapons development program office within the United States Marine Corps. The organization, referred to as *Program Office*, specializes in testing and evaluation of prototype weapon systems and relies heavily on information systems for office applications, test data collection, report creation, and historical information archiving. The resulting unique framework will set the stage for implementation of an effective Information Security (IS) governance program.

Discussion: Influencing Factors

As a Federal Government organization, several high level factors must be considered when creating the unique framework. Specifically, Congress has developed federal legislation defining legally accepted behavior and requires organizations to take specific steps to protect personal information. The Gramm-Leach-Bailey (GLB) Act "requires financial institutions to protect the confidentiality and integrity of the personal information of consumers" (Khoo, Harris, & Hartman, 2010). Additional legislation, such as the Sarbanes-Oxley Act (SOX), focuses on the financial sector where it supports "a simple premise: good corporate governance and ethical business practices are now required by law" (Khoo, Harris, & Hartman, 2010).

A substantial piece of federal legislation known as the Federal Information Security Management Act (FISMA) is an influencing factor which must be considered for the IS governance program. As discussed by Ely (2010), FISMA can be overwhelming and confusing to many organizations. With emphasis on mandatory monitoring, reporting, control testing, and many other areas, FISMA compliance has developed a form of "cottage industry" where expensive contractors offer assistance meeting the demands of the legislation and audit support. FISMA compliance is an overarching requirement that the *Program Office* must consider when developing their IS governance framework.

In response to the FISMA, the National Institute of Standards and Technology (NIST) developed a series of publications that will be important to the *Program Office's* IS governance program. Federal Information Processing Standards Publications (FIPS PUBS) are issued by

NIST and require Federal organizations to comply with outlined measures. For example, FIPS PUB 199 requires organizations to categorize their information systems in terms of potential impact should certain events occur. The impact level is assessed based off each security objective from FISMA – confidentiality, integrity, and availability (National Institute of Standards and Technology, 2004). Since the *Program Office* must be compliant with FISMA, the governance program will need to consider NIST's FIPS publications as a key component.

In addition to federal legislation, the IS governance framework should consider industry standards and accepted best practices for information security. While several organization's develop standards, one particular organization should be included in the *Program Office's* IS governance framework. The International Organization for Standardization (ISO) develops international standards enabling "a consensus to be reached on solutions that meet both the requirements of business and the broader needs of society" (International Organization for Standardization, 2011). Because the *Program Office* directly supports commercial weapons development programs, including ISO standards in the IS governance framework will increase interoperability between commercial developers and the government test and evaluation entity.

In addition to international standards, the *Program Office* governance framework will include many of the information security components identified by A. Da Veiga and J. H. P. Eloff (2007). Table 1 lists the security components that will be considered for implementation in the framework. Many of those security components were adapted from ISO standards, NIST publications, and the maturity models.

Another relevant consideration for development of the governance program is the role of continual process improvement and organizational process maturity. Several tools already exist which can help the organization achieve gains. The Information Technology Infrastructure

Library (ITIL) model offers a set of tools that the *Program Office* can leverage to implement best practices and promote higher service quality levels and cost optimization (MEGA international Ltd, 2005). Although a complete implementation of ITIL is often complicated, many of the components of ITIL will support the overall governance program and contribute to effective continual process improvement and organizational maturity.

In addition to ITIL, the Open Group Information Security Management Maturity Model (O-ISM3) offers to help organizations align Information Security Management (ISM) systems with the business mission and compliance needs. The O-ISM3 "delivers a process-based approach to information security management, and enables continuous improvement through the use of key security metrics" (The Open Group, 2011). The O-ISM3 is one of many maturity models. Research conducted by Roberto Saco (2008) estimates that between 100 to 200 different models are in existence today. Despite the varied approaches to measuring maturity, the best option is to use a combined strategy that takes pieces of different models with the goal of developing a unique model developed specifically for the *Program Office*. No one model will offer exactly what the *Program Office* needs.

Program Office Unique Framework

In developing the governance framework for the *Program Office,* the above discussed influencing factors were evaluated and organized into an overall implementable governance program. This framework is simply the starting point for the *Program Office* in implementing a breadth of governance programs. Overtime, the governance framework will need frequent review and revamping to keep current with business goals and environmental variables.

The fundamental basis for the *Program Office's* security governance framework is based from the work of Veiga & Eloff (2007). Adaptations were made to address the influencing factors mentioned earlier in this paper as they relate to the unique circumstances of the *Program Office*. The resulting framework consists of six pillars ranging from strategic level influences down to the technical level. A diagram is provided as Figure 1.

The first of six pillars is the Leadership pillar within the strategic realm of the organization. In order for the IS governance framework to work at the *Program Office*, the senior leadership (Colonels and Lieutenant Colonels) must support the initiatives and drive the program from top down. The Commanding Officer needs to sponsor the program giving the highest level endorsement stamp on the endeavor. In addition, the Chief Information Officer (CIO) must subscribe and make effort to develop an Information Technology governance program as the IS governance framework will interact with the IT program. Finally, the organization shall make use of business case documentation to drive capital decisions. Risk assessments and mitigation shall take place as part of the standard Risk Management Program (RMP) already in existence at the *Program Office*.

The second of the six pillars is the Security Management & Organization. This pillar falls within the managerial and operational realm and considers the high level concerns such as overall structure of the organization as it relates to information security. Laws such as FISMA and the Digital Millennium Copyright Act are included in the Legal & Regulatory component of this pillar.

The third of the six pillars is the IT Security Policies. This pillar falls within the managerial and operational realm where requirements from Department of Defense and United States Marine Corps Orders are considered. Best practices and guidelines are considered from various bodies of work including ITIL, FIPS, and the Defense Information Systems Agency's

(DISA) Security Technical Implementation Guides (STIG). The bulk of the *Program Office's* information security policies fall within this pillar of the overall IS governance framework.

The fourth of the six pillars is the Security Program Management. Monitoring the actions of employees and ensuring that technology is working as expected is an important part of the overall information security program. Monitoring allows for identification of anomalies and effective response to incidents (Veiga & Eloff, 2007). As discussed in the Influencing Factors section, FISMA contains continuous monitoring requirements and this pillar includes the needed compliance actions.

The fifth of the six pillars is the User Security Management. This pillar is the last of the managerial and operational pillars and considers user-related security components. User awareness helps develop a pro-security culture where the human aspect is considered and not just the technical controls. According to Experian's Chief Information Security Officer, "The human element is the largest security risk in any organization" (Kaplan, 2010). The emphasis of this pillar is to reduce the impact of the user on the overall security program by means of training, trust building, ethical conduct, and emphasis on privacy protection.

Lastly, the sixth of the six pillars is the Technology Protection and Operations. This pillar is the only technical level of the IS governance framework. This pillar focuses on keeping track of capital equipment, managing incidents, and addressing identified risks (Veiga & Eloff, 2007). Additionally, this pillar includes physical controls needed to safeguard equipment from loss and theft.

In addition to the components identified for each pillar, two components stretch across all levels (strategic, operational, and technical) of the framework. The configuration management and business continuity planning components are applicable to all levels of the framework and must be considered before any changes are implemented. The *Program Office's* Business Continuity Plan (BCP) falls within this component and is influenced by pieces of several other pillars of the framework, namely the policies requiring the plan and the need to continue operations based off mission requirements.

Conclusion

In conclusion, every organization has unique influences that should be considered when developing an information security governance program or framework. For the *Program Office,* the basic framework developed by Veiga and Eloff *(2007)* was adapted to meet the unique considerations imposed by federal legislation and Defense Department policies. Frameworks are broad and vague by nature and require further detail and customization to ensure successful implementation within various organizations. This case study paper identified the influencing factors and created a more specific framework ready for implementation. With ongoing adjustments throughout the life of the governance program, this framework can provide an effective information security governance program within the *Program Office.*

References

Bernard, S., & Ho, S. M. (2008). Enterprise Architecture as Context and Method for Designing and Implementing Information Security and Data Privacy Controls in Government Agencies.

Ely, A. (2010). 10 Steps To Ace A FISMA Audit. *Information Week*, 38-42.

International Organization for Standardization. (2011). *About ISO*. Retrieved 2 8, 2012, from ISO - International Standards for Business, Government and Society: http://www.iso.org/iso/about.htm

Kaplan, D. (2010, February 1). *Weakest link: End-user education.* Retrieved February 10, 2012, from SC Magazine: http://www.scmagazine.com/weakest-link-end-user-education/article/161685/

Khoo, B., Harris, P., & Hartman, S. (2010). Information Security Governance of Enterprise Information Systems: An Approach To Legislative Compliant. *International Journal of Management & Information Systems*, 49-55.

MEGA international Ltd. (2005, 11 9). MEGA International: MEGA ITIL accelerator helps IT departments optimise cost-effective quality of service, support and delivery. Coventry, UK.

National Institute of Standards and Technology. (2004, February). Standards for Security Categorization of Federal Information and Information Systems. Gaithersburg, MD.

Saco, R. (2008). Maturity Models: Inject New Life. *Industrial Management*, 11-15.

The Open Group. (2011, Apr 11). The Open Group Releases Maturity Model for Information Security Management: O-ISM3 Framework Ensures Security Management Processes Operate at a Level Consistent with Business Requirements. New York, NY, US.

Veiga, A. D., & Eloff, J. H. (2007). An Information Security Governance Framework. *Information Systems Management*, 361-372.

Table 1

*Information Security Components**

#	Title
1	Corporate governance
2	Information security strategy
3	Leadership in terms of guidance and executive level representation
4	Security organization
5	Security policies, standards, and guidelines
6	Measurement/Metric/Return on Investment
7	Compliance and monitoring
8	User management
9	User awareness
10	Ethical values and conduct
11	Privacy
12	Trust
13	Certification against a standard
14	Best practice and baseline consideration
15	Asset management
16	Physical and environmental controls
17	Technical operations
18	System acquisition, development, and maintenance
19	Incident management
20	Business continuity planning
21	Disaster recovery planning
22	Risk assessment process

* Excerpt from (Veiga & Eloff, 2007, p. 367)

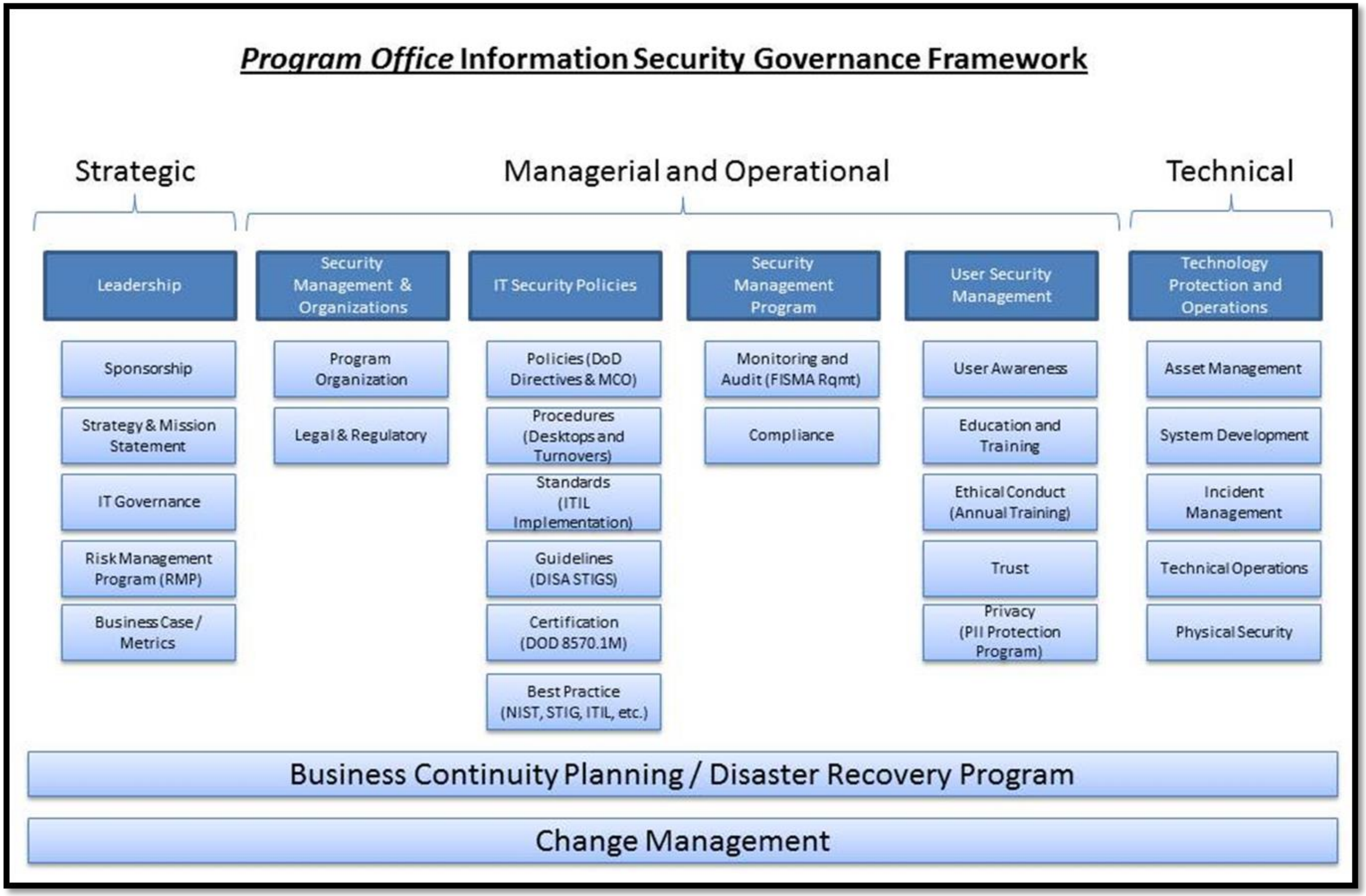
Program Office Information Security Governance Framework
Strategic
Managerial and Operational
Technical
Leadership
Sponsorship
Strategy & Mission Statement
IT Governance
Risk Management Program (RMP)
Business Case / Metrics
Security Management & Organizations
Program Organization
Legal & Regulatory
IT Security Policies
Policies (DoD Directives & MCO)
Procedures (Desktops and Turnovers)
Standards (ITIL Implementation)
Guidelines (DISA STIGS)
Certification (DOD 8570.1M)
Best Practice (NIST, STIG, ITIL, etc.)
Security Management Program
Monitoring and Audit (FISMA Rqmt)
Compliance
User Security Management
User Awareness
Education and Training
Ethical Conduct (Annual Training)
Trust
Privacy (PII Protection Program)
Technology Protection and Operations
Asset Management
System Development
Incident Management
Technical Operations
Physical Security
Business Continuity Planning / Disaster Recovery Program
Change Management

Figure 1. Program Office Information Security Governance Framework adapted from (Veiga & Eloff, 2007)

About the author

Author: Christopher Furton

Website: Http://christopher.furton.net

Certified professional with over 12 years of Information Technology experience and 8 years of hands-on leadership. An expert in cyber security with both managerial and technical skills proven throughout a career with increasing responsibility and performance expectations. Known ability to translate complex information for universal understanding. Detail-driven, results-focused leader with superior analytical, multitasking, and communication skills. Well-versed in industry best practices including Project Management and IT Service Management. Currently holding active CISSP, CEH, ITIL Foundations, Security+, and Network+ certifications.

Visit the auhor's blog:
IT Management Perspectives - https://christopherfurton.wordpress.com/

Social Sphere:

LinkedIn	Twitter	Google+	Quora	Wordpress	Flavors.me
Slide Share	Tumblr	YouTube	Pinterest	About.me	Vimeo