Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2010 Proceedings

Americas Conference on Information Systems (AMCIS)

8-2010

Security Management Life Cycle (SMLC): A Comparative Study

Joobin Choobineh
Texas A&M University, JChoobineh@mays.tamu.edu

Evan Anderson
Texas A&M University, Eanderson@mays.tamu.edu

Michael R. Grimaila
Air Force Institute of Technology, Michael.Grimaila@afit.edu

Security Management Life Cycle (SMLC): A Comparative Study

Joobin Choobineh
Information and Operations Management
Mays Business School
Texas A&M University
College Station, Texas 77843-4217
979-845-4048
Fax: 979-845-5653
(JChoobineh@mays.tamu.edu)

Evan Anderson
Information and Operations Management
Mays Business School
Texas A&M University
College Station, Texas 77843-4217
979-862-6515
Fax: 979-845-5653
(Eanderson@mays.tamu.edu)

Michael R. Grimaila
Center for Cyberspace Research
Air Force Institute of Technology
Wright Patterson AFB, OH USA
michael.grimaila@afit.edu

ABSTRACT

We introduce an integrated conceptualization of enterprise information technology security management in the form of a life cycle that accounts for the people, processes, infrastructure, and applications within an enterprise. Our life cycle view provides a lens through which one can view the security management activities at the strategic, tactical, and operational levels with regard to their strategic alignment with organizational goals. We compare and contrast three widely adopted frameworks (COSO, COBIT and ITIL) for enterprise risk and IT management with respect to our life cycle. We conclude that although the definitions of each stage of the life cycle are similar in these frameworks, their approach, philosophy, and method of execution is primarily determined by their unique focus. By developing a life cycle abstraction which encapsulates all of these frameworks, security management can better understand how their responsibilities and activities support organizational objectives.

Keywords

Security Management, Security Life Cycle, IT Management, COSO, COBIT, ITIL.

INTRODUCTION

Modern organizations are routinely faced with numerous types of risks. In some cases, the risks can be so serious as to threaten the existence of the organization. These risks include financial, market, competitive, regulatory, and operational risks. A significant component of operational risk is that of violation of security of the organization. This includes both physical (e.g., buildings and facilities), logical (e.g., process violations), and information technology (IT) security breaches. Various frameworks and guidelines have been proposed for managing overall risk. Perhaps the most widely adopted one is the Committee of Sponsoring Organizations (COSO) which provides guidance on critical aspects of organizational governance, business ethics, internal control, enterprise risk management, fraud, and financial reporting (Beasley et al. 2009, IIA 2005, Simmons 1997). Similarly, multiple frameworks have been proposed for the management of IT. Most include guidelines for the management of IT security. The two most widely used frameworks for IT management are Information Technology Infrastructure Library (ITIL) (OGC 2006, OGC 2007a-f) which is focused on quality IT service delivery and Control Objectives for Information and related Technology (COBIT) (COBIT 2007) which is focused on IT governance.

In this paper, we formulate a clear set of requirements for effective management of IT security in section 2. In section 3, we introduce our life cycle view of the management of security. Using elements of the life cycle, in section 4 we compare and contrast these frameworks. We conclude the paper in section 5 and propose future research.

REQUIREMENTS FOR EFFECTIVE MANAGEMENT OF SECURITY

We opine that effective management of security must contain at least the following three characteristics: 1) focus on impact on business objectives, 2) life cycle view of security, and 3) integrated analysis of security and controls across the strategic, tactical, and operational levels of the organization.

The requirement for focus on impact on business objectives is best put forth in the widely adopted International Organization for Standardization (ISO) Information Security Management document:

> *"…development of a security policy, objectives and activities that reflect business objectives; implementing security that is consistent with the organizational culture; obtaining visible support and commitment from management; a good understanding of the security requirements, risk assessment and risk management; effective marketing of security to all managers and employees; distribution of guidance on information security policy and standards to all employees and contractors; providing appropriate training and education; and a comprehensive and balanced system of measurement which is used to evaluate performance in information security management and feedback suggestions for improvement." (*ISO/IEC 17799 2005)

The first clause in this statement is of paramount importance. The ultimate goal of security management must be to support business objectives. Hence, our premise is that all other aspects of security management should evolve around the support of business objectives. This implies careful attention to not only analysis of risks associated with resources but also to propagation of those risks to processes that utilize the resources and ultimately to business objectives that are fulfilled by the processes (ITGI 2005). Similarly, National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30 "Risk Management for Information Technology Systems" states, "*The principal goal of an organization's risk management process should be to protect the organization and its ability to perform their mission, not just its IT assets*" (Stoneburner et al. 2002). Organizations must understand how their business objectives are impacted by losses of resources critical to success of their mission.

The current best practice and literature tends to focus on the protection of resources (ISSA 2010, INFOSEC 2010, I^2SF 2010, $(ISC)^2$ 2010, and OCTAVE 2010). Our position is different in that we explicitly recognize that resources contribute differently to business objectives. In particular, we recognize that the contribution of each resource is neither necessarily proportional to its own cost nor to the significance of each of the objectives that it supports. The protection of resources is an intermediate step of the overall goal to ensure that the business objectives are protected from delays or even complete failure to achieve.

The argument for a life cycle view can be inferred from the widely adopted ITIL best practices as quoted below:

> "*Insufficient attention is given to the active management of information security, the continuous analysis and translation of policies into technical options and ensuring that the security measures continue to be effective when requirements and environments change.*" *(*OGC 2006)

The keywords in this quote are "*continuous analysis*." Continuous analysis begs for a life cycle view of the management of security. Here, as in many other places, change is the only constant. A life cycle view assures continued effectiveness in the face of ephemeral requirements changes as a result of changes in the environment.

Integrated analysis across strategic, tactical, and operational levels refers to the fact that each level of the organization should be carefully managed for security. Ignoring any of these levels could lead to missing important aspects of analysis and sub optimization. More importantly, the analysis should include the boundaries between these levels and not be viewed as three different and unrelated analyses. ITIL recognizes this fact and warns of the consequences of ignoring the link between organizational levels when considering security management:

> *"… The consequence of this missing link between the strategic and the tactical level is that, at the tactical management level, significant investments are made in measures that are no longer relevant, at a time when new, more effective measures ought to be taken. Security Management aims to ensure that effective Information Security measures are taken at the strategic, tactical and operational levels." (OGC 2006)*

LIFE CYCLE VIEW OF THE MANAGEMENT OF SECURITY

In Figure 1, we provide an integrated conceptualization of enterprise security management. The square box within the figure contains the life cycle itself. The top part of the figure represents the impact on organization. The first level of impact is on business units and their tasks. The units and their tasks fulfill organizational objectives. Hence, the second level is on the objectives of the organization at each of the three levels of strategic, tactical and operational.

Four elements are at the heart of the life cycle. These are people, processes, infrastructure and applications. People refers to the various stakeholders, their proxies, or their representatives. Processes represent the management activities that are undertaken to govern the operations of the organization. Infrastructure refers to the components of the organization that enable delivery of IT services to people. It includes hardware, system software, data and knowledge bases, buildings, and utilities. Applications are software or aggregation thereof that uses the infrastructure to provide IT services to the people.

The life cycle itself consists of five phases. These are Risk Assessment, Policy Definition, Requirements Delineation, Establishment of Controls, and Environmental Monitoring (Anderson, R. 2001, Bennet and Kailay 1992, COBIT 2007, I2SF 2010, IIA 2005, ISO/IEC 2005, OCTAVE 2010, OGC 2007a, Rees et al. 2003). The solid arrows from one phase to the next collectively signify the life cycle process. The dashed arrows indicate the iterative process and feedback through the loop.

Assess Risk. The purpose of this step is to inform the management of the potential impact on organizational objectives of various threats given certain controls in the presence of certain vulnerabilities. This step is initiated because of one of two events. The first is a predetermined schedule to conduct an internal audit. The second is due to one or more internal or external environmental changes. Internal environmental changes occur because of changes in objectives, acquisitions of recourses, and changes in controls. External environmental changes are due to emergence of new threats, enactment of new laws, directives from governmental authorities having jurisdiction over the organization, or identification of new opportunities in controlling risks.

Define Policy. Security policy is a set of high level definitions of constraints on the behavior of the internal system components as well as those that could be imposed on the actions of potential adversaries. Based on the assessment results, existing policies, guidelines, and procedures are *reviewed*, *updated* if needed, and *created* if non-existent. The updated or newly created policies must iteratively be validated until gaps are filled, contradictions resolved, and duplications eliminated. At each iteration, the new or updated security policies must be mapped to pertinent assessment results to assure their alignment with organizational objectives. The process must be participatory embracing all the stakeholders including top management, affected units within the organization, and the security professionals.

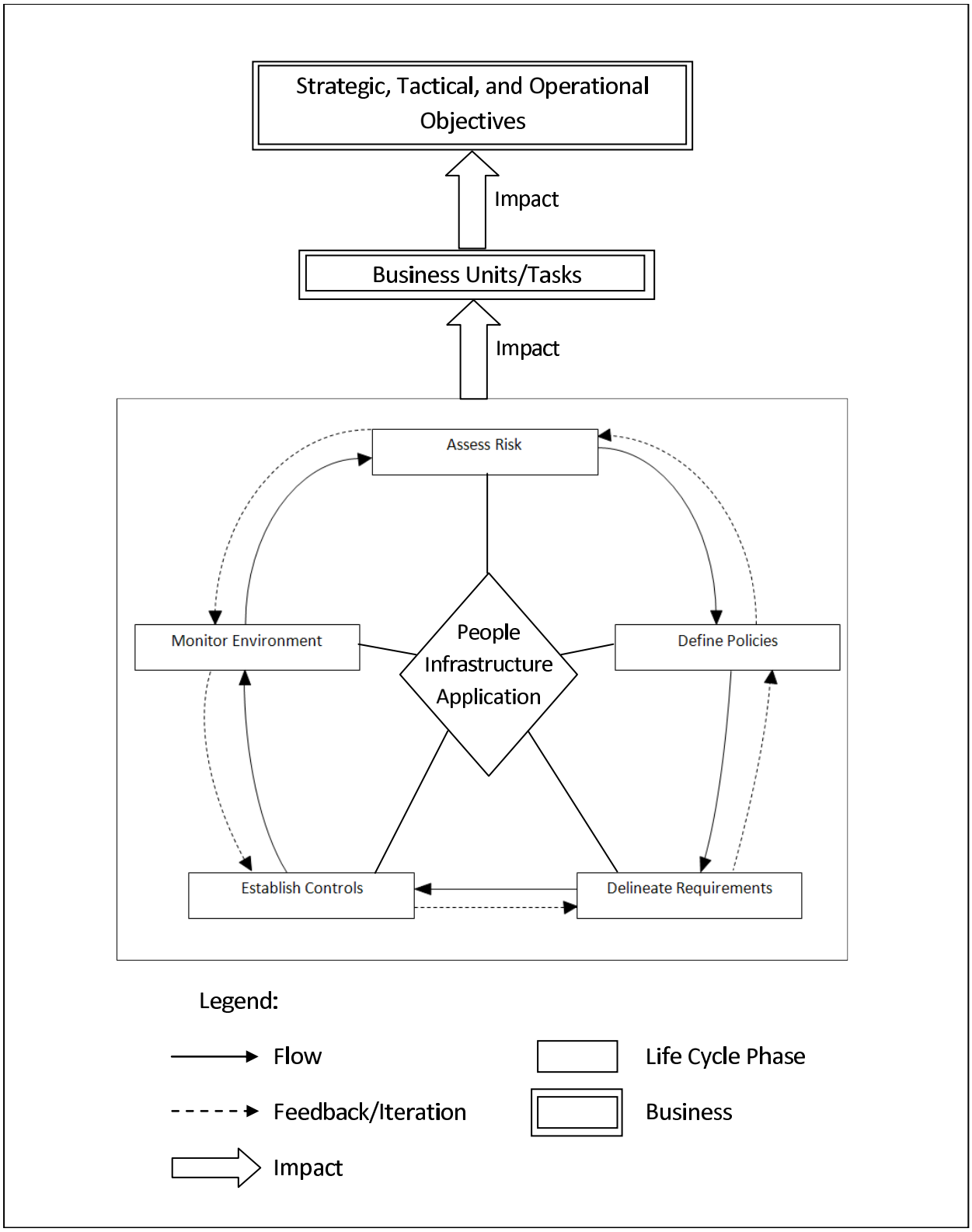

Figure 1. Security Life Cycle and its Impact

Delineate Requirements. Based on the defined policies, a set of security requirements are developed. These are procedures, methods, and their levels that are necessary for the protection of people, infrastructure, and applications. The requirements are organized in a hierarchical structure where a more abstract higher-level node is broken down into its details. The depth and the breadth of the requirements is a function of the size of the organization and its mission(s). For instance, an organization within the defense establishment will have a more extensive set of requirements than a similar size organization in a non-defense industry. At the highest level of the hierarchy are the desired levels of protection of *physical* resources, *non-physical* assets, and *personnel*. Specifications of the requirements must take into account security best practices, specific practices within the market segment of the organization, laws and regulations of the jurisdictions within which the organization is operating, and the unique socio-technical environment of the organization itself. Once completed, the requirements must be validated against the set of defined policies and revised if needed.

Establish Controls. Controls are management practices where tools, resources, and techniques are utilized to prevent, detect, and correct harmful and undesirable events. Requirements are implemented through new or modification of the existing controls. If new controls are required, then alternatives must be evaluated and selections be made. New controls are then *designed*, *implemented,* and *tested* to assure satisfaction of the requirements.

Monitor Environment. This is the steady state of securing the organization through controls. The *internal* environment is monitored for undesirable events, compliance with the policies, and identification of new vulnerabilities. Violations of compliance are communicated to affected stakeholders and recommendations for appropriate actions are made. Occurrence of an unforeseen event would necessitate update of the security database and initiation of risk assessment. Likewise, the *external* environment is monitored for identification of new threats and new controls. Environmental changes are fed back through the loop to modify controls, requirements, and policies. Major changes will necessitate risk assessment.

COMPARISON OF COSO, COBIT, AND ITIL: SECURITY MANAGEMENT PERSPECTIVE

In this section, we provide an analysis and comparison of three of the more widely used risk management and IT frameworks with respect to the management of information security and relative to the life cycle model presented earlier. These are COSO, COBIT, and ITIL. COSO provides a framework for the management of all risks to the organization including financial risks. COBIT is an IT governance framework which explicitly links organizational goals to the underlying business and IT processes. ITIL's perspective is that of providing a framework for management of the delivery of IT services. A brief summary of each is presented next.

COSO

COSO establishes a high level enterprise risk management framework that is based on information flows, risk governance that defines roles and responsibilities, and assurance procedures and control for the mitigation of risk. Fundamentally, it seeks to create a template for risk identification, assessment of impacts and the implications for organizational objectives. Information flows from bottom to top and top to bottom, with responsibilities and actions dispersed throughout the organization.

The most fundamental objective of COSO is to inform senior executives and Boards of Directors of the risk that are involved in all aspects of organizational activities, relationships, and environments. It is created at a sufficiently high level that every organization can fit within it. A fundamental tenet of COSO is that senior management and the Board of Directors are ultimately responsible for the fulfillment of objectives, that conditions of risk may negatively impact objectives and that organizational leadership must act, based on informed judgment, to dispense with risks by accepting them or to mitigate them through institutional means such as insurance or through internal controls.

Senior management, given its responsibility for achieving organizational objectives and for the protection of stakeholders' interest, must digest the implications of risks and strike a tolerable balance between those it will accept and those that it will mitigate. If risks are to be mitigated by internal controls, senior management must provide the leadership and resources for those activities and create processes, procedures, and reporting requirements that assure the presence and effectiveness of controls.

Information technologies are both sources of risk and means of mitigation. While COSO does not prescribe detailed guidance for security architecture nor configuration best practices, it establishes information technologies as a source of controls and as an enabler for data collection and information management about control assurance.

COBIT

Control Objectives for Information and related Technology (COBIT) is a business focused, strategic Information Technology (IT) governance framework that enables management to explicitly link business goals to IT goals, provides metrics and maturity models to measure their achievement, and identifies the associated responsibilities of business and IT process owners (COBIT 4.1, 2007). COBIT was developed to address management concerns regarding the pervasive embedding of IT into critical business processes, increasing regulatory compliance requirements, and the desire to provide a well documented and transparent means for managing IT related risks. COBIT is a control based framework that drives IT policy and implementation of best practices by defining sets of control objectives, application controls, process controls, and performance measurements necessary to assure that the management of IT is strategically aligned with the organizations business objectives.

The COBIT framework is aligned with COSO's Internal Control Integrated Framework and employs five major governance focus areas: Strategic Alignment, Value Delivery, Resource Management, Risk Management, and Performance Measurement. COBIT defines four domains that are used to control, manage, and measure each of the 34 COBIT defined core IT processes. First, a high-level control objective is defined for each process. It includes a) a process description summarizing the process objectives, b) a high-level control objective represented as a waterfall that summarizes process goals, metrics and practices, and c) a mapping of the process to the COBIT process domains, information criteria, IT resources and IT governance focus areas. Second, a detailed set of control objectives for the process is defined. Third, a set of management guidelines are documented including the process inputs and outputs, a RACI (Responsible, Accountable, Consulted and/or Informed) chart, and the process goals and metrics. Finally, the maturity level of the process is determined so that opportunities for process improvement can be identified and progress over time can be tracked.

COBIT provides a well structured framework for the collection and analysis of the information required to rationally manage IT in view of the organizational objectives. COBIT supports IT governance by providing a framework to ensure that IT is aligned with the business, IT enables the business and maximizes benefits, IT resources are used responsibly, and IT risks are managed appropriately.

ITIL

ITIL (Information Technologies Infrastructure Library) was developed in the late 1980s as a set of guidelines for the UK government with the goal of effective management of information technologies. Over time, its mission evolved into that of guidelines for delivery of quality IT services. Since its inception, the motivation has been the realization of the tremendous dependence of organizations on IT services. Although hard data is lacking, but a simple Google search on the words "ITIL" and "standard" reveals that many in the industry believe that ITIL is the *de facto* global standard for information technology management. It is owned by OGC (Office of Government Commerce, Great Britain) but is free to public. (See OGC 2006 through OGC 2007-f). ITIL contains two main areas: Service Support and Service Delivery.

Service support is focused on delivering quality and continuous service to the users. It consists of the following management activities: 1) Incident Management (restoring services as soon as possible), 2) Problem Management (finding the underlying cause of the incidents and proposing solutions), 3) Change Management (evaluation of the impact on IT infrastructure due to changes), 4) Release Management (implementation of changes), and 5) Configuration Management (record keeping and periodic audit of IT configuration). The five management activities are supported by two important functions: The service desk that logs and monitors the incidents and a knowledge base of information needed for proper discharge of the activities.

Service delivery is focused on the quality and cost effective execution of the delivery of IT services. The main function of service delivery is Service Level Management. It focuses on achieving the service level agreement and quality. It is supported by a Configuration Management Database (CMDB) that contains information on hardware software items as well as their physical and logical interrelationships. Four other functions support service delivery. These are: 1) Availability Management (continuous availability and reliability), 2) Capacity Management (planning for and monitoring capacity), 3) Financial Management (cost benefit analysis and measurement of quality/cost ratio), 4) Continuity Management (evaluation of risks, planning for contingencies, and recovery from serious incidents.)

Comparison

In Table 1 we provide a summary and a comparison of the three widely adopted IT management frameworks relative to our Security Management Life Cycle (SMLC) with a narrow focus on the management of security.

At the highest level, each framework is distinguished from another on its focus. That is, its domain of attention and its breadth relative to organizations' functions. Following the presentation of the target audience, we present a summary of each of the frameworks (ITIL, COSO, and COBIT) relative to the five stages of the SMLC. To a great extent, the focus of each of the frameworks determines their approach and their view of the five phases of the life cycle.

Risk Assessment - The definition of risk assessment in SMLC, ITIL, and COBIT are similar and is limited to the IT risk. COSO has the broadest view of risk in that it assesses all risks to the organization.

Policy Definition - In ITIL, policy definition is included as part of the planning process for security management. In both COSO and COBIT, policy definition is established by the highest level of management.

Requirements Delineation - Service Level Agreements (SLA) are a very important consideration in ITIL. As a result, SLAs form the fundamental basis for delineation of requirements. In COSO, the amount of mitigated risk relative to tolerated risk derives the delineation of the requirements. COBIT has a similar process to ITIL with the exception that process owners play a significant role in the delineation.

Establishment of Controls - ITIL views controls as consisting of two parts. One is the management of controls and the other is their implementation. COSO focuses on internal controls with little attention to IT. COBIT, being business process focused, lets the business process owners establish controls for specific business activities.

Monitoring of Environment – ITIL divides this into two components. "Evaluate" is the internal and external audits as well as self assessments. "Maintain" is the continuous learning and quality improvement as a result of the audits and self assessments. COSO's monitoring is primarily through periodic audits focusing on the internal environment. COBIT has a separate phase, "Monitor and Evaluate" to verify policy compliance and validate requirements.

SUMMARY, CONTRIBUTIONS AND FUTURE RESEARCH

In this paper, we argued for the need to view the management of IT security as a life cycle of its components with the ultimate goal of measuring the impact of breaches on organizations' strategic, technical, and operational objectives. The life of the management of security starts with assessment of risks followed by stages of policy definition, requirements delineation, control establishment, environmental monitoring and back to risk assessment. The five stages of life cycle must embrace a holistic and all encompassing approach to the security of people, infrastructure, and applications. Within this life cycle view, we compared and contrasted three widely used risk and IT management frameworks. Although the definitions of each of the stages of the life cycle are similar in these frameworks, their approach, philosophy, and method of execution of each stage of the life cycle is primarily determined by their unique focus.

Contributions

This study has made a few contributions. First, it is the first study that puts security management within a dynamic life cycle perspective. The traditional framework models such as COSO, COBIT, and ITIL are static. The advantages of a dynamic life cycle model include its explicit representation of feedback loops and the clarity with which the perpetual characteristic of the security management work is revealed. Second, the use of the model enables identification of gaps in security management across the three levels (Strategic, Tactical, and Operational) of an organization with their sometimes conflicting objectives. (See Figure 1 and the row labeled "*Focus*" in Table 1.) Third, the emphasis on measuring impact on the tasks and eventually the objectives of each of the three levels (Strategic, Tactical, and Operational) enables focus on the most important aspect of organizational management; that is, the objectives. Fourth the comparison between the existing frameworks (COSO, COBIT, and ITIL) within the life cycle view reveals the hierarchical relationship, in order from COSO to ITIL, between them resulting in the potential of the model to be used in organizations that employ these frameworks to further enhance their security management function.

Table 1 – Mapping of the Security Management Life Cycle (SMLC) to ITIL, COSO, and COBIT Frameworks

		SMLC	COSO	COBIT	ITIL
Focus		Security Management	Enterprise Risk Management	Enterprise IT Governance.	Management of IT Services
Target Audience		All three levels of the org.	Board & Executives	Board & Executives	IT Organizations
Elements of the Life Cycle	**Risk Assessment**	Enterprise-wide identification of sources of risk, likelihood and impacts.	Identification of 7 types of risks: enterprise deployment, acquisition, implementation, operational, requirements and policy compliance risks.	Measurement of the potential impact on organizational objectives of various threats given certain controls in the presence of certain vulnerabilities.	Similar to SMLC. Viewed as part of the more general function of Business Continuity Management.
	Policy Definition	Expresses organization's appetite for risk. Requires Board of Directors oversight.	Is established by executive management during the Plan and Organize phase.	A set of high level definitions of constraints on the behavior of the internal system components and adversaries.	Included as part of "*Plan*" for security management.
	Requirements Delineation	Requirements must be approved by the Board of Directors and senior management. The amount of tolerated risk relative to mitigated risk is determined.	Control requirements are derived jointly by process owners and IT management.	A set of security requirements to achieve enforcement and execution of policies.	Labeled "*Plan*". Service Level Agreements determine most of it. Internal policies are added.
	Establishment of Controls	The focus is primarily on internal controls. Very little specific attention is given to the use of information technologies to manage access to or protection of information assets.	At the business process level, controls are established and applied to specific business activities.	Implementation of requirements through management practices where tools, resources, and techniques are utilized to prevent, detect, and correct harmful and undesirable events.	Divided into two components: "*Control*" refers to management organization and responsibilities. "*Implement*" refers to technical implementation of security and resolution of incidents.
	Monitoring of Environment	Primarily internal. Largely focused on assurance that controls are deployed as required. Audits are periodic to insure that the Board's risks are managed to acceptable levels.	The Monitor and Evaluate phase encompasses all of the activities necessary to validate requirements and verify policy compliance.	Monitoring of the internal and external environments to assure compliance with policies and repeat of the life cycle.	Divided into two parts: "*Evaluate*" refers to internal and external audits and self assessments. "*Maintain*" refers to learning and improvement of the current system.

Future Research

We have three specific plans for future research. First, we intend to study and to provide further details of the mappings between the SMLC model and each of the COSO, COBIT and ITIL frameworks. Second, we intend to include the relevance of the Capability Maturity Model Integration (CMMI) to SMLC. A key feature of CMMI, which is well-aligned with our study, is its focus on explicit linkage between the tasks of business processes with organizational objectives. (See Figure 1.) A more challenging future research is the development of metrics that can measure the robustness of security management within the life cycle framework.

ACKNOWLEDGMENTS

This work was sponsored in part by research grants from Cisco Systems, Inc. Critical Infrastructure Assurance Group, Texas A&M University (Center for Information Assurance and Security and Center for the Management of Information Systems), the Air Force Research Laboratory, and the Air Force Institute of Technology (Center for Cyberspace Research).

DISCLAIMER

The views expressed in this paper are those of the authors and do not reflect the official policy or position of the United States Air Force, the Department of Defense, or the U.S. Government.

REFERENCES

1. Anderson, R., "Why Information Security is Hard – An Economic Perspective," IEEE Proc. of the 17th Annual Comp. Security Applications Conference, pp. 358-365, 2001.

2. Beasley, M.S., Hancock, B. V. and Branson, B. C. (2009). Strengthening Enterprise Risk Management for Strategic Advantage, Committee of Sponsoring organization of the treadway Committee, www.coso.org.

3. Bennet, S.P. and Kailay, M.P., "An Application of Qualitative Risk Analysis to Computer Security for the Commercial Sector," IEEE Proceedings of the Eighth Annual Computer Security Applications Conference, pp. 64-73, 30-November-4 December 1992.

4. COBIT - Governance, Control and Audit for Information and Related Technology, IT Governance Institute / ISACA / ISACF, 4th edition (2007).

5. I2SF (International Information Security Foundation), available as of April 26, 2010 http://www.opengroup.org/security/more.htm.

6. IIA, Putting COSO theory into Practice (November, 2005) Tone at the Top, Institute of Internal Auditors.

7. INFOSEC Assurance Training and Rating Program (IATRP), "INFOSEC Assurance Capability Maturity Model (IA-CMM) Version 3.1," November 2004, available as of April 26, 2010 at http://www.isatrp.org/

8. (ISC)2 International Information System Security Certification Consortium, Inc., "Common Body of Knowledge (CBK)," available as of April 26, 2010, at http://www.isc2.org

9. ISO/IEC 17799:2005, "ISO/IEC Information Technology - Code of Practice for Information Security Management." ISO/IEC 17799, 2005.

10. ISSA (Information Systems Security Association), "Generally Accepted Information Security Principles V3.0 (GAISP)," available as of April 26, 2010 at http://all.net/books/standards/GAISP-v30.pdf.

11. ITGI, "Information System Risks: Whose Business Are They Anyways?" IT Governance Institute, 2005.

12. OCTAVE, "Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)," OCTAVE CERT Coordination Center, Software Engineering Institute at Carnegie Mellon University; available as of April 26, 2010, at http://www.cert.org/octave/

13. OGC (2006) Planning to Implement Service Management, The Stationary Office, London.

14. OGC (2007-a) Introduction to ITIL, The Stationary Office, London.

15. OGC (2007-b) Service Design, The Stationary Office, London.

16. OGC (2007-c) Service Improvement, The Stationary Office, London.

17. OGC (2007-d) Service Operation, The Stationary Office, London.

18. OGC (2007-e) Service Transition, The Stationary Office, London.

19. OGC (2007-f) The Official Introduction to the ITIL Service Life Cycle, The Stationary Office, London.

20. Rees, J., Bandyopadhyay, S., and Spafford, E.H. PFIRES: A Policy Framework for Information Security. Communications of the ACM. 46, 7. July 2003, 101-106.

21. Simmons, M. R. (1997) COSO Based Auditing, The Internal Auditor, 54, 6, 68-73.

22. Stoneburner, G, Goguen, A., and Feringa, A. "Risk Management Guide for Information Technology Systems," National Institute of Standards and Technology Special Publication 800-30, 2002.