CONF-IRM 2015 Proceedings

International Conference on Information Resources Management (CONF-IRM)

5-2015

IT Security Governance: A Framework based on ISO 38500

Suchit Ahuja
Queen's School of Business Queen's University, Kingston, Canada, suchit.ahuja@queensu.ca

Yolande E. Chan
Queen's School of Business Queen's University, Kingston, Canada, ychan@queensu.ca

P46. IT Security Governance: A Framework based on ISO 38500

Suchit Ahuja
Queen’s School of Business
Queen’s University, Kingston, Canada
suchit.ahuja@queensu.ca

Yolande E. Chan
Queen’s School of Business
Queen’s University, Kingston, Canada
ychan@queensu.ca

Abstract

ISO 38500 is an international standard for IT governance. The guidelines of ISO 38500 can also be applied at the IT security functional level in order to guide the governance of IT security. This paper proposes the use of a strategic information security management (ISM) framework to implement guidelines of ISO 38500. This approach provides several strategic advantages to the organization by 1) aligning IT security initiatives to business strategy; 2) providing a mechanism for establishing and tracking security metrics; and 3) enhancing the overall maturity of business, IT and IT security processes. The framework also leverages tools such as COBIT, the Balanced Scorecard and SSE-CMM in order to implement IT security governance and continuous improvement practices. Using extant literature, this paper identifies certain challenges and solutions with respect to the governance of IT security. For practitioners, it highlights relevant links between principles of ISO 38500 and IT governance, provides an over-arching contextual framework to drive IT security governance, and demonstrates mitigation solutions for IT security governance challenges. For academics, the paper makes theoretical contributions, by relating IT security governance to business strategy and proposing that firms develop dynamic governance capabilities (Pavlou and El Sawy, 2010) or organizational learning ladders (Ciborra and Andreu, 2010).

Keywords

ISO 38500; COBIT; Balanced Scorecard; SSE-CMM; Governance; Information Security Management; IT Security Metrics; Business/IT Alignment

1. Introduction

As firms increasingly leverage IT for driving business growth, gaining competitive advantage, and enabling strategic differentiation, the management and governance of IT is gaining greater importance due to the growing complexity of both the business organization and its systems and technologies (Gordon, Lee and Lucas, 2005). In such a complex scenario, one of the biggest challenges for the IT organization is the protection of information assets, prevention of intellectual property theft, and safeguarding the privacy of employees and customers. IT security is gaining increasing importance within organizations, as security threats escalate (Sipior and Ward, 2008). Data theft and breaches from cybercrime have cost businesses as much as $1 trillion globally in lost intellectual property and expenditures for repairing the damage (Ponemon Institute, 2014). Recent high profile security breaches, such as those at Target, JPMorgan Chase, and Home Depot, have highlighted the importance of IT security for businesses. Furthermore, a recent survey by the Ponemon Institute (2014) showed the average cost of cybercrime for U.S. retail stores more than doubled from 2013 to an annual average of $8.6 million per company in 2014.

One main reason for the existence of weaker security mechanisms has been that firms tend to attribute too much importance to the technical aspects of IT security and only superficially address the management aspects. The focus of information security is generally more towards deploying technical tools and systems instead of using a comprehensive framework that includes people, processes, technology, procedures and policies (Pironti, 2006; Siegel, Sagalow, and Serritella, 2003). However, IT security is no longer a technology-focused problem and it has become the basis for business survival as much as any other issue (DHS, 2013). IT security has risen to the level of the C-suite or board as an issue of critical concern (Deloitte, 2007). According to the IT Governance Institute (2007a), boards of directors are increasingly expected to make information security an intrinsic part of governance, integrated with processes they already have in place to govern other critical organizational resources. Thus, IT security has moved from being an operation management issue to an enterprise-level governance issue.

IT security governance requires a framework predicated on principles and accountability requirements that encourage desirable behavior in the application and use of technology (Deloitte, 2007). This involves establishing and maintaining a framework and supporting management structure and processes to provide assurance that information security strategies: 1) are aligned with and support business objectives; 2) are consistent with laws and regulations through adherence to policies and internal controls; and 3) provide assignment of responsibility to all in order to manage risk (DHS, 2013). Accordingly, any IT security governance framework must include components of alignment, compliance, and accountability. This is difficult to achieve because of the lack of standards-based IT security governance mechanisms. Although there are several ongoing efforts towards standardization of IT governance, organizations face numerous implementation challenges (IT Governance Institute, 2007a). It is also difficult to establish clear top-down "traceability" (Goldman and Ahuja, 2009) for IT security decisions and track relevant metrics (Johnston and Hale, 2009; Krahmann, 2003; Von Solms, 2005).

In this paper, we use the ISO 38500, an international standard for the corporate governance of information and communication technology (38500.org, 2008), to demonstrate how governance of IT security can be achieved using principles of ISO 38500 in conjunction with Information Security Management (ISM). With respect to practical contributions, we highlight relevant links between principles of ISO 38500 and IT governance, provide an over-arching contextual framework to drive IT security governance, and demonstrate mitigation solutions for IT security governance challenges. We also make theoretical contributions by linking IT security governance to business strategy and proposing that firms develop dynamic governance capabilities (Pavlou and El Sawy, 2010) or organizational learning ladders (Ciborra and Andreu, 2010).

Past studies have highlighted the importance of governance of the ISM function from a strategic standpoint (Da Cruz and Labuschagne, 2006; IT Governance Institute, 2007c; Von Solms, 2005). The low success rate of ISM programs across various organizations can be attributed to the lack of corporate governance of information security and a lack of clarity in terms of ownership of digital assets. Digital information is a valuable and critical corporate asset, and it is imperative for the corporate board to assume direct responsibility and accountability for information security. Sarbanes Oxley (SOX) compliance highlights the fact that the boards of publicly listed firms are held directly responsible and accountable for financial audits (Hall and Liedtka, 2007).

According to previous research, a single framework for ISM generally proves inadequate for purposes of strategic IT security governance and most frameworks tend to focus more heavily on technical aspects of security rather than governance (Posthumus and Von Solms, 2004; Siponen and Oinas-Kukkonen, 2007). This paper draws attention to governance aspects by using the ISO 38500 internationally recognized framework for IT governance and showing how components of ISM can be leveraged to achieve IT security governance. This paper also serves as a response to a call for future research in the IT governance area using COBIT (Control Objectives for Information and Related Technology) as a framework (De Haes, Van Grembergen, and Debreceny, 2013). We provide a top-down and end-to-end view of the use of COBIT components in conjunction with other frameworks such as the Balanced Scorecard and the Systems Security Engineering Capability Maturity Model (SSE-CMM), in the context of IT security and following ISO 38500 principles.

In order to demonstrate the usefulness of combining ISO 38500 with ISM for IT security governance, we highlight the alignment of IT security initiatives with business strategy, the establishment and tracking of relevant security metrics, and enhancement of the overall maturity of security processes. Without a robust governance mechanism, ISM lacks strategic direction, thereby only enabling the organization to fulfill regulatory compliance requirements or to enforce and manage IT security controls. Therefore, we combine ISM with a governance framework to strengthen "IT security governance" and enhance decision-making capabilities.

2. Defining the Artifacts and Context

In this section, the over-arching framework of ISO 38500 is highlighted with respect to its core principles and implementation guidelines. Next a definition of "IT governance" is provided which is then extrapolated to "IT security governance". Finally, the strategic ISM framework is described and its components comprising COBIT, the Balanced Scorecard (BSC) and SSE-CMM are discussed.

2.1 ISO 38500

ISO 38500 is an international standard for IT Governance. It sets out six principles for good corporate governance of IT that express preferred behavior to guide decision making – responsibility, strategy, acquisition, performance, conformance, and human behavior. ISO 38500 recommends that 1) plans and policies must be established at the corporate level for guiding IT projects; 2) proposals for IT improvements and new undertakings must originate at the project and operational level, but must be reported for evaluation to corporate management; 3) performance and conformance of IT projects is the responsibility of the corporate board; 4) business needs must be clearly identified and evaluated for any IT project; and 5) the corporate board is responsible for direction, evaluation, and monitoring of all IT entities (see Figure 1). Based on these recommendations, IT security governance addresses the following (DHS, 2013):

- Security is managed as an enterprise issue and executive leaders understand their accountability and responsibility for IT security for the organization and its stakeholders.
- Security is treated as a business requirement and security policy is set at the top of the organization with input from key stakeholders.
- Security has achievable, measurable objectives that are integrated into strategic and project plans and implemented with effective controls and metrics.
- Security is addressed strategically and as part of any new project initiation, acquisition, or relationship and as part of ongoing project management. All personnel who have access to digital assets and enterprise networks understand their individual responsibilities with respect to protecting and preserving the organization's security.

Previous research indicates that ISO 38500 is not "one size fits all" and must be customized to fit the firm's IT environment and requirements. It is designed to be complementary to COBIT, IT Infrastructure Library (ITIL), or other standards or frameworks by providing a demand-side-of-IT-use focus (Sylvester, 2011). Although ISO 38500 provides guidance about IT governance via its principles and recommendations, it does not indicate "how" firms can implement those guidelines by augmenting them with complementary frameworks. Furthermore, it does not provide specific tools that can be applied or processes that can be implemented (Lewis, 2008). In this paper, we address this issue by providing specific examples of the integration of ISO 38500 with some complementary frameworks. Nonetheless, organizations must decide on specific tools and frameworks depending on scale, maturity of processes, domain of business, etc. In this paper, we use the tools provided by the ISM framework such as COBIT, BSC, and SSE-CMM for this purpose.

2.2 The ISM Framework

According to Siponen and Oinas-Kukkonen (2007), "Information Security Management refers to a means of maintaining secure IS in organizations, including IS planning and evaluation. This also includes the questions of backup, recovery, and contingency management. Confidentiality, availability, integrity, and non-repudiation are the requirements for security management". In order to ensure the strategic orientation of ISM, the processes and components that drive the management of IT security must be combined within a strategic framework. To meet this challenge, within the context of this paper, we use a strategic ISM framework (Goldman and Ahuja, 2011). This framework depicts several important aspects of the above definition of ISM. The components of the framework will be used as tools to implement the guidelines of ISO 38500. The goal is to focus on the utility of the components with respect to IT security governance. A brief description of the critical components follows.

2.2.1 COBIT

By definition, COBIT is an IT governance framework and supporting toolset that allows managers to bridge the gap between control requirements, technical issues and business risks (IT Governance Institute, 2007b). According to the IT Governance Institute (2007a), COBIT enables clear policy development and good practice for IT control throughout organizations. COBIT emphasizes regulatory compliance, helps organizations in increasing the value attained from IT, and enables business/IT alignment (Debreceny, 2006; Larsen et. al., 2006; Ridley, Young, and

Carroll, 2004). Within the context of the ISM framework, COBIT is an important component because most of the process-level implementation of business initiatives and control mechanisms (more than 200 process controls) are covered under domains of COBIT (with each domain consisting of several specific processes).

2.2.2 Balanced Scorecard (BSC)

The Balanced Scorecard (Kaplan and Norton, 1996) is a performance management system that enables businesses to drive strategies based on goal definitions (Van Grembergen and De Haes, 2005). The BSC approach usually consists of four specific domains: 1) Financial Perspective; 2) Internal Business Process Perspective; 3) Customer Perspective; and 4) Learning and Growth Perspective. For this paper, the domains can be repurposed to fit the requirements of IT security strategy. To align Business, IT, and IT Security strategies, we use a cascading BSC approach in the ISM framework. According to the Balanced Scorecard Institute (2008), "cascading a balanced scorecard means to translate the corporate-wide scorecard (referred to as Tier 1) down to first business units, support units or departments (Tier 2) and then teams or individuals (Tier 3)". The organizational alignment should be visible throughout the strategic plan, with the help of strategy maps, performance measures, performance targets, and initiatives.

2.2.3 Systems Security Engineering Capability Maturity Model (SSE-CMM)

The Systems Security Engineering Capability Maturity Model (SSE-CMM) is a tool for engineering organizations to evaluate security-engineering practices and to define performance improvements (SSE-CMM.org, 2009). SSE-CMM provides a model that is useful in assessment of the level of security maturity in an organization's systems, regardless of the methodology used to implement the systems, thereby making it "methodology neutral" (Goldman and Christie, 2004).

In the rest of the paper, we address: 1) Major challenges with respect to governance of IT security; 2) relevant links between principles of ISO 38500 and IT governance; 3) an over-arching contextual framework to drive IT security governance using ISO 38500 and COBIT; and 4) solutions to the identified challenges using components of a strategic ISM model.

3. Challenges in IT Security Governance

A survey of IT governance literature reveals important challenges outlined below.

3.1 Governance of Information

The lack of a well-defined information classification mechanism within the organization often results in weak governance of information (Bacik, 2008). This can lead to unclear information-asset ownership, increased cost of information protection due to lack of a clear expenditure strategy, redundancy in IT security processes, and complexities in enabling mitigation mechanisms. For ISM purposes, the most commonly used tool for classifying information assets is an Information Classification Matrix (ICM) (Burkett, 2012; Sherwood, Clark and Lynas, 2005). With ICM, the standard for classification of information is to assign a rating of High (H), Medium (M), or Low (L) for each criterion within an information category. These should ideally be provided by an "information governance" committee that uses business drivers as a guideline.

3.2 Alignment between Business/IT and IT Security Strategies

There is lack of processes that enable the implementation of initiatives for realizing business-level goals with respect to IT security (Goldman and Ahuja, 2009). Although the definition of goals, objectives and metrics is clear at the business and IT levels and their applicable processes areas are known, there is still a gap in terms of conversion of the IT-level initiatives into initiatives and metrics to the IT security entity of the organization.

3.3 Lack of an Enterprise IT Security Maturity Model

Firms often use a combination of frameworks to address business, IT and IT security management, thereby making governance even more challenging. Firms encounter several challenges trying to integrate these frameworks (Ozkan, Hackney and Bilgen, 2007). It is difficult to derive an "enterprise-wide maturity model" for security governance, risk, and compliance.

3.4 IT Security Auditing

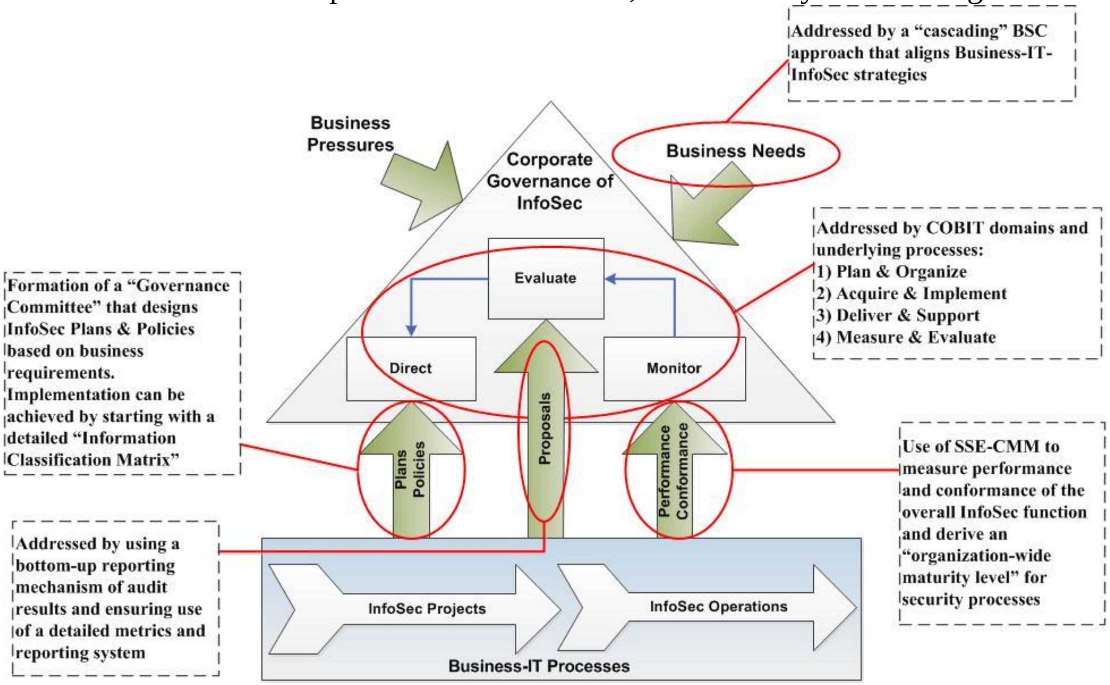
With respect to ISM, the result of an audit is usually a major driver for reporting and compliance improvements (Chapin and Akridge, 2005). Consequently, key metrics defined for IT security processes and systems are tracked, reported and updated via dashboards. While reporting "IT security performance" independently from IT performance or operational performance, an incomplete assessment might be projected (Geffert, 2004; Goldman and Christie, 2004). This can result in ineffective top-down security implementation and process improvement. Thus, organizations face challenges with respect to IT security governance. Table 1 shows the challenges identified above and provides logical mappings to the six principles of ISO 38500 with further "drilled-down" mappings to broad IT Governance Areas from ISO 38500. This establishes a vital link between governance of IT security and ISO 38500. It also serves as an over-arching conceptual umbrella, under which a comprehensive model for IT security governance can be established.

Challenges in IT security governance	**ISO 38500 Principles**	**IT Governance Areas**
3.1 Governance of Information	Responsibility, Conformance Acquisition	Risk Management (RK) Resource Management (RM)
3.2 Alignment between Business/IT and IT security Strategies	Strategy, Performance, Conformance	Strategic Alignment (SA) Risk Management (RK) Value Delivery (VD) Performance Measurement (PM)
3.3 Lack of an enterprise IT security maturity model	Performance, Conformance	Risk Management (RK) Value Delivery (VD) Performance Measurement (PM)
3.4 Audit and IT security reporting problems	Performance, Conformance, Human Behavior	Risk Management (RK) Performance Management (PM)

Table 1: IT Governance Mapping

4. Mitigation of IT Security Governance Challenges

In this section, potential solutions for mitigation of the aforementioned challenges will be discussed. Firstly, these solutions are adopted from individual components of the ISM framework and help in enabling IT security governance. Secondly, two of the most important components that will be used are COBIT and ISO 38500. It is therefore imperative to ensure that these components are linked to each other, so that they can together drive the security governance processes. Appendix A maps ISO 38500 principles to COBIT processes within each COBIT domain. This provides clarity in tracking each process to its logical origin for IT security governance purposes, and establishes a relevant cross-referencing between processes of COBIT Domains and ISO 38500. Next, Figure 1 shows a model for IT security governance, which was designed by adapting ISO 38500 for "IT Security". This is an important contribution of this paper as it establishes a framework for IT security governance, based on an internationally recognized standard of IT governance. In Figure 1, the red circles highlight "challenges in IT security governance" which were also highlighted in Table 1. These IT security governance challenges will be addressed using the mechanisms mentioned in the dotted boxes. It is important to note that due to page length limitations, we have only provided high-level details of these mitigation mechanisms. Moreover, these mechanisms consist of several interlinked processes and metrics at the strategic, tactical, and operational levels. In order to meet the page length limitations and to provide a clear and concise snapshot of the framework, we have only included high-level details.



Addressed by a "cascading" BSC approach that aligns Business-IT-InfoSec strategies

Addressed by COBIT domains and underlying processes:
1) Plan & Organize
2) Acquire & Implement
3) Deliver & Support
4) Measure & Evaluate

Formation of a "Governance Committee" that designs InfoSec Plans & Policies based on business requirements. Implementation can be achieved by starting with a detailed "Information Classification Matrix"

Use of SSE-CMM to measure performance and conformance of the overall InfoSec function and derive an "organization-wide maturity level" for security processes

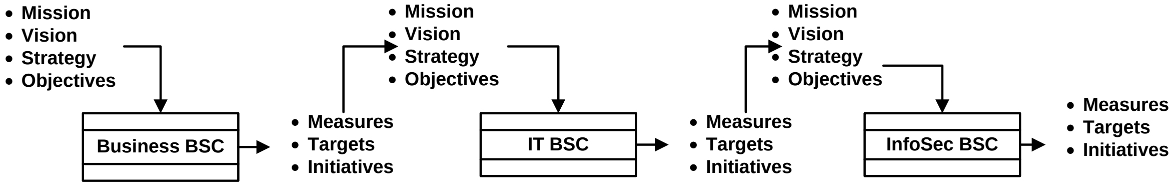
Addressed by using a bottom-up reporting mechanism of audit results and ensuring use of a detailed metrics and reporting system

Figure 1: IT Security Governance framework adapted from ISO 38500

4.1 Business Needs: Aligning Business/IT and IT Security Strategies

We begin by addressing the ISO 38500 recommendation of factoring in business needs for IT security governance. Although the COBIT process area "Plan and Organize (PO1)" requires the establishment of a strategic IT plan, it does not provide tools to deploy the strategic IT plan.

As shown in Figure 2, a cascading BSC approach can be adopted to address this gap. The use of a cascading BSC establishes alignment between the business strategy (based on business processes and information), IT strategy, and IT security strategy (Rouyet-Ruiz, Spauwen, and Aguila, 2010), thereby enabling the extrapolation of a unified strategy across the organization from the



executive management level to the operational security level (Goldman and Ahuja, 2011). The cascading BSC approach usually consists of tiers, with each tier addressing the strategy, objectives, measurements, targets and initiatives at different business units within the organization (usually hierarchical, i.e., business, IT within business, and IT security within IT).

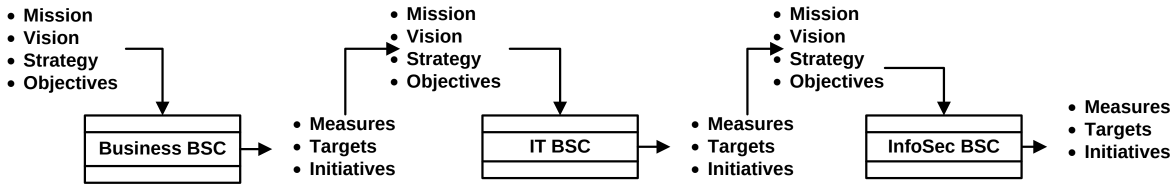
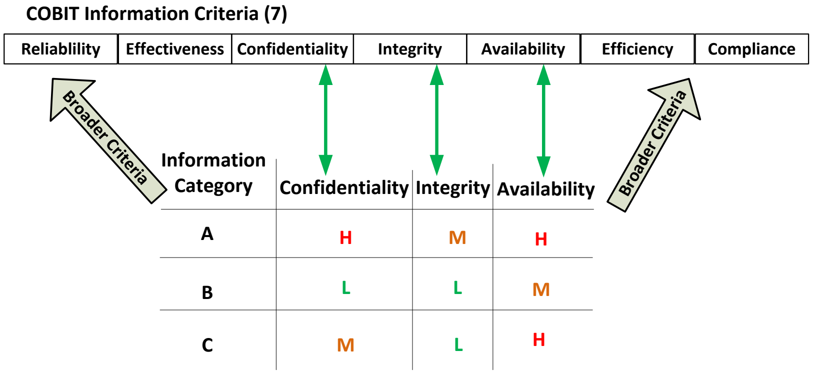


Figure 2: Cascading BSC approach for strategic alignment

4.2 Plans and Policies: Governance of Information

One of the major problems with existing information classification tools is that they are not granular enough to accommodate growing complexities of information assets (Baars and Spruit, 2012; Garigue, 2007; Hsiao et al., 2014). In order to resolve this we use COBIT Information Criteria (shown in Figure 3) for effective classification of information, based on a clear set of criteria as defined by an IT Governance Committee, leading to lower risks and avoidance of conflicts between executive management (Blair, Watt and Cull, 2010).



Information Category	Confidentiality	Integrity	Availability
A	H	M	H
B	L	L	M
C	M	L	H

Figure 3: Information Governance via use of COBIT Information Criteria

4.3 Lack of an Enterprise IT Security Maturity Model

ISO 38500 recommends the usage of mechanisms to track IT success and operational failures. Within the IT security context, this is challenging. Ad hoc adoption of individual maturity models for measuring processes within different functions of the organization can result in flawed assessments. As a solution, we suggest the combined use of methodologies specified by Goldman and Christie (2004), Mallette (2005), IT Governance Institute (2007a), and IT Governance Institute (2008) to facilitate development of an enterprise-wide IT security maturity model. This approach creates mappings between COBIT domains and SSE-CMM process areas (Figure 4), such that the organization can streamline common functions and processes that need to be tracked in order to achieve efficient ISM.

Once an enterprise-wide security maturity model is established, the flow of information between operational level security, managerial level security and strategic security must be ensured.

Organizations engage in regular audits for this purpose, but the audits are performed at systems or operational and managerial levels. However, for effective governance the results of these audits must flow to the governance committee and top management. We address this issue next.

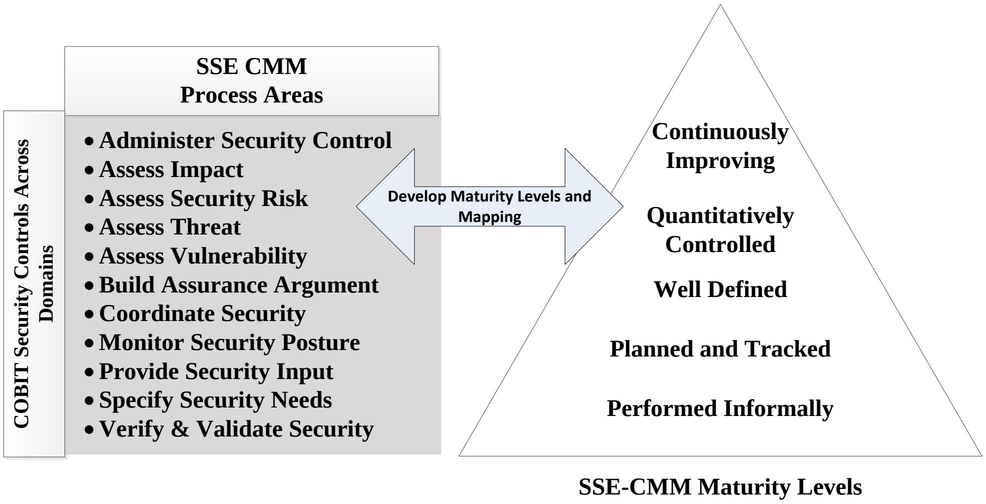


Figure 4: SSE-CMM and COBIT security processes and maturity levels

4.4 Audit and IT Security Reporting Problems

In order to ensure "traceability" (Goldman and Christie, 2004) and conversion effectiveness (Weill, 1992) between business goals and technical security processes, valid and relevant metrics must be reported to the IT Governance Committee. A comprehensive mechanism that reports such metrics needs to be established (see Figure 5). The flow of security-related information originates at the operational and project levels of IT security. Key Performance Indicators (KPIs) and Key Goal Indicators (KGIs) are used. This permits the meaningful reporting of security data directly to the business level, thereby contributing towards the conversion effectiveness of investments in operational security controls (Goldman and Ahuja, 2009, 2011).

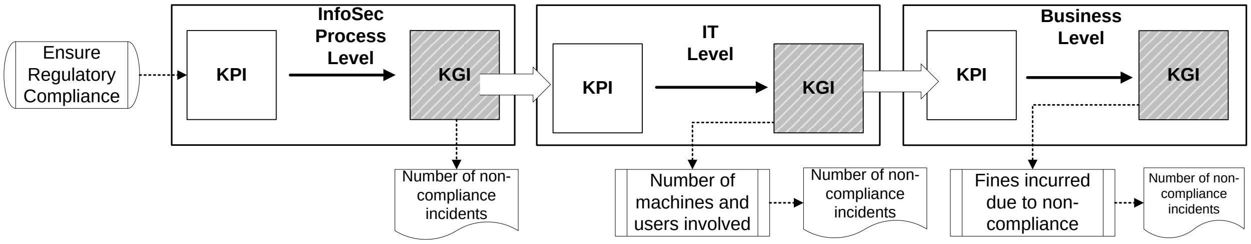

Ensure Regulatory Compliance
InfoSec Process Level
KPI
KGI
IT Level
KPI
KGI
Business Level
KPI
KGI
Number of non-compliance incidents
Number of machines and users involved
Number of non-compliance incidents
Fines incurred due to non-compliance
Number of non-compliance incidents

Figure 5: KPI-KGI and InfoSec metrics

In summary, a model for IT security governance has been designed using the international IT governance standard (ISO 38500), with the context re-framed to make it relevant to "IT security". The unique contributions of this paper are: 1) identification of major challenges with respect to governance of IT security using existing literature; 2) establishment of relevant links between principles of ISO 38500 and existing IT governance areas; and 3) creation of an over-arching contextual framework to drive IT security governance using ISO 38500 and COBIT.

Moreover, we have gone beyond the “prescriptive recommendations” of ISO 38500 to also provide usable frameworks, tools and mechanisms for both academics and practitioners.

5. Conclusion and Implications

The goal of this paper was to display how IT security governance can be facilitated via the application of principles of ISO 38500, using tools provided by a strategic ISM framework. We address governance issues in IT security, showing how guiding principles of ISO 38500 can be used. Finally, we combine the components of ISM such as COBIT, BSC, and SSE-CMM, to show how strategic IT Security Governance can be formulated. This serves as a step towards the use of existing frameworks and standards for the purpose of IT Security Governance.

Practitioners can gain insights regarding implementation challenges, standardized processes, and IT security governance solutions. Thus, starting at the resource-level of IT security operations, a clear strategic governance mechanism can be established. Academics can view this approach from the lens of creating dynamic governance capabilities (Pavlou and El Sawy, 2010) or organizational learning ladders (Ciborra and Andreu, 2010). The principles of ISO 38500 form capabilities and the components provide the routines and work practices, thereby strengthening the overall core capability of the organization in terms of IT security governance. These two views (dynamic capabilities and learning ladders) can be explored in future research.

References

38500.org (2008) “ISO 38500 IT Governance Standard”, *International Standards Organization*, http://38500.org/index.htm (current January 29, 2015).

Baars, Thijs, and Marco Spruit. (2012). "Analysing the Security Risks of Cloud Adoption Using the SeCA Model: A Case Study." *J. UCS* 18, no. 12 : pp. 1662-1678.

Bacik, S. (2008) *Building An Effective Information Security Policy Architecture*. Boca Raton, FL: CRC Press.

Balanced Scorecard Institute [BSCI] (2009) “About - Balanced Scorecard”, http://www.balancedscorecard.org/BSCResources/AbouttheBalancedScorecard/tabid/55/Default.aspx (current December 12, 2014).

Blair, S., R. Watt, T. Cull (2010) “Responsibility-driven Architecture”, *Software IEEE*, 27(2), pp. 26-32.

Burkett, J. S. (2012) “Business Security Architecture: Weaving Information Security into Your Organization's Enterprise Architecture through SABSA®”, *Information Security Journal: A Global Perspective*, 21(1), pp. 47-54.

Chapin, D. A. and S. Akridge (2005) “How can Security be Measured”, *Information Systems Control Journal*, 2, pp. 43-47.

Ciborra, C. U. and R. Andreu (2001) “Sharing Knowledge Across Boundaries”, *Journal of Information Technology*, 16(2), pp. 73-81.

Da Cruz, E. and L. Labuschagne (2006) “A New Framework For Bridging The Gap Between IT Service Management and IT Governance from a Security Perspective”, http://icsa.cs.up.ac.za/issa/2005/Proceedings/Full/072_Article.pdf (current January 15, 2015).

Debreceny, R.S. (2006) “Re-engineering IT Internal Controls: Applying Capability Maturity Models to the Evaluation of IT Controls”, *Proceedings of the 39th Hawaii International Conference on System Sciences*, 2006. IEEE.

De Haes, S., W. Van Grembergen, R. S. Debreceny (2013) “COBIT 5 and Enterprise Governance of Information Technology: Building Blocks and Research Opportunities”, *Journal of Information Systems*, 27(1), pp. 307-324.

Deloitte Touche Tohmatsu (2007) “2007 Global Security Survey”, http://www.deloitte.com/assets/Dcom-Shared%20Assets/Documents/dtt_gfsi_GlobalSecuritySurvey_20070901.pdf (current January 29, 2015).

Department of Homeland Security [DHS] (2013) “Security Is Not Just a Technical Issue”, *Build Security In*, https://buildsecurityin.us-cert.gov/articles/best-practices/governance-and-management/security-is-not-just-a-technical-issue (current January 29, 2015).

Garigue, R. (2007). "Understanding the New Information Risks: The Requirement for a New Information Security Conceptual Framework." *EDPAC: The EDP Audit, Control, and Security Newsletter* 35, no. 3: pp. 1-9.

Geffert, B. T. (2004) “Incorporating HIPAA Security Requirements Into An Enterprise Security Program”, *Information Systems Security*, 13(5), pp. 21-28.

Goldman, J.E. and S. Ahuja (2009) “Integration of COBIT, Balanced Scorecard and SSE-CMM as a Strategic Information Security Management (ISM) Framework”, *Proceedings of the Fourth International Workshop on Business/IT Alignment and Interoperability (BUSITAL'09)*, Amsterdam, Netherlands.

Goldman, J. E. and S. Ahuja (2011) “Integration of COBIT, Balanced Scorecard and SSE-CMM as an Organizational and Strategic Information Security Management (ISM) Framework”, in Quigley, M (ed.), *ICT Ethics and Security in the 21st Century: New Developments and Applications*, Hershey, PA: Information Science Reference, pp. 277-309. doi:10.4018/978-1-60960-573-5.ch014.

Goldman, J.E. and V.R. Christie (2004) “Metrics based Security Assessment”, in Quigley, M (ed.), *Information Security and Ethics: Social and Organizational*, IRM Press, pp. 261-287.

Gordon, J. R., P. M. Lee, H. C. Lucas (2005) “A Resource-Based View Of Competitive Advantage At The Port Of Singapore”, The Journal of Strategic Information Systems, 14(1), pp. 69-86.

Hall, J. A. and S. L. Liedtka (2007) “The Sarbanes-Oxley Act: implications for large-scale IT outsourcing”, *Communications of the ACM*, 50(3), pp. 95-100.

Hsiao, D. K., Douglas S. Kerr, and Stuart E. Madnick. (2014). *Computer Security*. Academic Press, 2014.

IT Governance Institute (2007a) “COBIT Mapping: Mapping SEI’s CMM for Software with COBIT 4.0”, http://www.isaca.org/Template.cfm?Section=COBIT_Mapping1andTemplate=/ContentManagement/ContentDisplay.cfmandContentID=27170 (current January 29, 2015).

IT Governance Institute (2007b) “COBIT 4.1 Handbook”, http://ww.itgi.org (current December 15, 2014).

IT Governance Institute (2007c) “Information Security Governance: Guidance for Information Security Managers”, http://www.itgi.org (current January 23, 2015).

IT Governance Institute (2008) “Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit”, http://www.itgi.org (current December 10, 2014).

Johnston, A. C. and R. Hale (2009) “Improved Security Through Information Security Governance”, *Communications of the ACM*, 52(1), pp. 126-129.

Kaplan, R.S. and D.P. Norton (1996) “Using the Balanced Scorecard as a Strategic Management System”, *Harvard Business Review*, January-February, 1996.

Krahmann, E (2003) “Conceptualizing Security Governance”, *Cooperation and Conflict*, 38(1), pp. 5-26.

Larsen, H. M., K. M. Pedersen, V. K. Viborg Andersen (2006) “IT Governance – Reviewing 17 IT Governance Tools and Analysing the Case of Novozymes A/S”, *Proceedings of the 39th Hawaii International Conference on System Sciences*, 2006. IEEE.

Lewis, E. (2008) “Principles and the Governance of IT”, In the *Proceedings of the 19th Australasian Conference on Information Systems*, pp. 03-05.

Mallette, D. (2005) “IT Performance Improvement with COBIT and SEI CMM”, *Information Systems Audit and Control Association ISACA,* http://www.isaca.org (current January 15, 2015).

Ozkan, S., R. Hackney, S. Bilgen (2007) “Process Based Information Systems Evaluation: Towards The Attributes of PRISE”, *Journal of Enterprise Information Management,* 20(6), pp. 700-725.

Pavlou, P. A. and O. A. El Sawy (2010) “The “Third Hand”: IT-enabled Competitive Advantage in Turbulence Through Improvisational Capabilities”, *Information Systems Research*, 21(3), pp. 443-471.

Ponemon Institute (2014) “2014 Cost of Cyber Crime Study: United States”, *Hewlett Packard,* https://ssl.www8.hp.com/us/en/ssl/leadgen/document_download.html?objid=4AA5-5208ENW (current January 29, 2015).

Posthumus, S. and R. Von Solms (2004) “A Framework for the Governance of Information Security”, *Computers and Security*, 23(8), pp. 638-646.

Pironti, J.P. (2006) “Information Security Governance: Motivations, Benefits and Outcomes”, *Information Systems Control Journal*, 4, pp. 45-48.

Ridley, G., J. Young, P. Carroll (2004) “COBIT and its Utilization: A Framework from the Literature”, *Proceedings of the 37th Annual Hawaii International Conference on System Sciences*, 2004. IEEE

Rouyet-Ruiz, J., W. Spauwen, L. Aguilar (2010) “Using COBIT 4.1 to Achieve Business-IT Alignment: A Practical Approach*”, ISACA Journal Online*, 1(1).

Sherwood, J. A. Clark, D. Lynas (2005) *Enterprise Security Architecture: A Business-Driven Approach*. Taylor and Francis Group.

Siegel, C. A., T. R. Sagalow, P. Serritella (2003) “Cyber Risk Management”, *Information Security Management Handbook*, pp. 829-836.

Sipior, J. C. and B. T. Ward (2008) “A Framework for Information Security Management Based on Guiding Standards: A United States Perspective”, *Issues in Information Science and Information Technology*, 5, pp. 51-60.

Siponen, M. T. and H. Oinas-Kukkonen (2007) “A Review of Information Security Issues and Respective Research Contributions”, *ACM Sigmis Database*, 38(1), pp. 60-80.

SSE-CMM.org (2009) “How Secure is SSE-CMM?”, http://www.secure-software-engineering.com/2008/02/19/how-secure-is-sse-cmm/ (current December 21, 2014).

Sylvester, D. (2011) "ISO 38500—Why Another Standard?." *COBIT Focus* 2 (1).

Van Grembergen, W. and S. De Haes (2005) “Measuring and Improving IT Governance Through The Balanced Scorecard”, *Information Systems Control Journal*, 2(1), pp. 35-42.

Von Solms, B. (2005) “Information Security Governance: COBIT or ISO 17799 or both?”, *Computers and Security*, 24(2), pp. 99-104.

Weill, P. (1992) “The Relationship Between Investment in Information Technology and Firm Performance: A Study of the Valve Manufacturing Sector”, *Information Systems Research*, 3(4), pp. 307-333.

Appendix A – Mapping ISO 38500 Principles with Logical COBIT Processes Across All COBIT Domains

<table>
<tr><th colspan="7">ISO 38500 Principles</th></tr>
<tr><th rowspan="10">COBIT Processes Across Domains</th><th>Responsibility</th><th>Strategy</th><th>Acquisition</th><th>Performance</th><th>Conformance</th><th>Human Behaviour</th></tr>
<tr><td>PO4: Define the IT processes, organization and relationships</td><td>PO1: Define the strategic IT plan</td><td>PO5: Manage the IT investment</td><td>PO2: Define the information architecture</td><td>PO4: Define IT processes, organization and relationships</td><td>PO4: Define the IT processes, organization and relationships</td></tr>
<tr><td>PO6: Communicate management aims and direction</td><td>PO2: Define the information architecture</td><td>PO10: Manage projects</td><td>PO5: Manage the IT investment</td><td>ME1: Monitor and evaluate IT performance</td><td>PO7: Manage IT Human Resources</td></tr>
<tr><td>PO7: Manage IT Human Resources</td><td>PO3: Determine the technology direction</td><td>AI1: Identify automated solutions</td><td>PO6: Communicate management aims and direction</td><td>ME2: Monitor and evaluate internal control</td><td>AI4: Enable operational use</td></tr>
<tr><td>DS2: Manage third-party services</td><td>PO5: Manage the IT investment</td><td>AI2: Acquire and maintain application software</td><td>PO8: Manage quality</td><td>ME3: Ensure regulatory compliance</td><td>DS1: Define and manage service levels</td></tr>
<tr><td>ME1: Monitor and evaluate IT performance</td><td>PO10: Manage projects</td><td>AI3: Acquire and maintain technology infrastructure</td><td>PO9: Assess and manage IT risks</td><td></td><td>DS7: Educate and train users</td></tr>
<tr><td>ME4: Provide IT Governance</td><td>AI1: Identify automated solutions</td><td>AI5: Procure IT resources</td><td colspan="3" rowspan="2">AI4: Enable operational use
Al6: Manage changes
DS2: Manage third-party services
DS3 – DS13* <b><i>(see below)</i></b> and ME4: Provide IT Governance</td></tr>
<tr><td colspan="3">AI7: Install and accredit solutions and changes
DS1: Define and manage service levels
DS2: Manage third-party services</td></tr>
<tr><td colspan="6"><b>*</b>DS3: Manage performance and capacity; DS4: Ensure continuous service; DS5: Ensure system security; DS6: Identify and allocate costs; DS7: Educate and train users; DS8: Manage service desk and incidents; DS9: Manage the configuration; DS10: Manage problems; DS11: Manage data; DS12: Manage the physical environment; DS13: Manage operations</td></tr>
</table>