Exploring the Role of Frameworks & Methodologies in Information Security Management & Governance - Research in Progress

Sharon W. Tabor

Boise State University, stabor@boisestate.edu

Follow this and additional works at: http://aisel.aisnet.org/amcis2009

Recommended Citation
http://aisel.aisnet.org/amcis2009/522

This material is brought to you by the Americas Conference on Information Systems (AMCIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in AMCIS 2009 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.
Exploring the Role of Frameworks & Methodologies in Information Security Management & Governance – Research in Progress

Sharon W. Tabor
Boise State University
stabor@boisestate.edu

ABSTRACT
IT governance and Information Security Management (ISM) are currently topics of great interest to practitioners and researchers alike. In reaction to financial fraud at major US companies, organizations are facing legal pressures and ongoing scrutiny of their overall governance processes, with efforts increasingly driven by the IT organization. ISM practice is also evolving, to help organizations strengthen security governance and develop a security culture that can address increasing internal and external threats. Organizations are showing interest in various formal methodologies as reference frameworks for their efforts, and expect the right choice to enhance both IT and security governance. The ultimate choice, however, must fit the organization context and risk profile, and ISM frameworks are only workable if organizations derive value from them.

Keywords (Required)

INTRODUCTION
Following the Enron and WorldCom scandals of 2001 that impacted financial markets, resulted in the dismantlement of a major accounting firm, and left employees without pension funds, efforts to mandate corporate governance through legislation have put considerable attention on how organizations are being managed. Information technology units are stepping into the role of enabler to strengthen the oversight of corporate governance through better management and security of corporate data. However, when economic performance is down and budgets are tight, it is not unusual for information technology departments to come under scrutiny and face budget cuts. This cyclical tightening activity seems to follow major economic declines such as the oil crisis of the early 1980’s, savings and loan and real estate declines in the late 1980’s and early 1990’s, the dotcom bust of the new millennia, and the current global economic crisis starting in 2007.

An important defense to IT cutbacks is for business-oriented IT leadership to make sure they are involved strategically with organizational goals and directions, that they employ practices that optimize the efficient use of IT assets, and set policies that address risk levels relevant to organizational assets and requirements. This research in progress paper is part of an interpretive study on how governance in general and more specifically, ISM practice has developed and evolved in organizations through the use of frameworks and methodologies. This portion of the study examines the choices and expectations that challenge IT management when considering the adoption of an appropriate framework, how they gauge their current maturity level with security practice adoption, and what value they felt was derived from their implementation.

BACKGROUND LITERATURE
The literature in the area of information security is growing, although as noted by Siponen and Oinas-Kukkonen (2007), much of it to date has been concerned with the technical and operational aspects of security. This is to be expected, as organizations of all sizes face growing challenges of protecting their data assets against both internal and external threats, and insuring the traditional security goals of confidentiality, integrity, and availability (CIA) are achieved. Further work is needed, however, to examine how organizations can develop a security culture through policies and principles relevant to their view of security risk and mitigation and move toward the broader concept of security governance. To accomplish this broader view Dhillon and Backhouse (2000) suggest the traditional technical goals of CIA need to be further expanded to include social components of responsibility, integrity, trust, and ethicality. These expanded goals can further efforts to achieve security governance, where organizational relationships and processes for managing risk are clearly defined, implemented, measured, and regularly reassessed. Additionally, this approach helps address concerns expressed by Wylder (2004) that organizations have a fixation on the technical view of information security.
Information Security Management (ISM) practice as a field is also evolving, moving toward the identification of security management practices that will balance security process with proper management oversight. ISM research to date has leaned toward a concentration on policy, guidelines, and contingency management. To further mature in this area, von Solms (2005b) suggests organizations should develop separate, yet complementary ISM functions to distinguish operational security management from security compliance management, therefore insuring that security governance receives independent oversight from those performing security management tasks. In practice, organizations are struggling with choosing the right framework that will enhance operations without contributing extra overhead or result in resistant from end users.

THE JOURNEY TO SECURITY GOVERNANCE

In 2004, CIO magazine published results of a survey of 100 IT executives from companies chosen based upon their excellent IT reputation. The premise of the article was that if chief information officers (CIOs) are to achieve the goal of demonstrating IT value, they must run their IT organizations more like the business of which they are a part. To accomplish this goal and also the higher and often elusive goal of alignment with business strategy, the article suggests there might exist some common ‘best of breed’ IT practices that can create a foundation for success. While some argue that the term “best practice” has no meaning, it is widely used in IT organizations, and typically represents an effort to benchmark current organizational practice against operating practices of high achieving organizations or other set of commonly accepted practices or frameworks. Technically oriented IT literature has extensively addressed the value of tactical methods such as checklists and standards, labeled by Siponen as “normative management-oriented security standards” (2003, p.1550). Best practices as used in this paper, however, are considered to be process-oriented, if not strategic, views of activities that should be done to reach a successful conclusion.

It is likely that a single framework or methodology may not suffice for all organizations. While some industries have specific legal requirements, i.e., HIPAA privacy requirements for healthcare, that guide their governance efforts, others may find one or more well recognized methodologies necessary and appropriate to address governance and security in their organization. For example, von Solms suggests the blending of COBIT with ISO 17799 (now 27001) as a broader based solution for security governance (2005a). Whatever terminology is adopted, the goal of continuous improvement is a noble one, and badly needed to help IT organizations demonstrate value to their organizations and achieve appropriate levels of both IT and security governance. If existing frameworks help organizations achieve their goals, then valuable resources need not be used to reinvent proven processes.

IT governance evolves as a direct effect of improvement efforts, and is specifically about the management of the organization’s technology assets, including the need to insure that scarce resources are used for technology investments that will add value to the organization, to identify who the decision-makers are, to specify on what criteria the decisions should be made, and direct how the decisions will be implemented. Weill and Ross (2004) refine the definition of IT governance as “specifying the decision rights and accountability framework to encourage desirable behavior in using IT” (p.2). Efforts to develop strong information security governance practice were further fueled by the need to meet compliance deadlines for security, integrity, and privacy mandated in Sarbanes-Oxley, Gramm-Leach-Bliley, and HIPAA legislation. In this case, while compliance was expensive, legislation helped organizations receive funding to enhance their security profile that might otherwise have been more difficult to obtain.

Information security governance (ISG) is a less researched area of the overall corporate and IT governance domain, and has been identified variously by different authors. It fits in well with the broader definition of IT governance, emphasizing the CIA goals. Efforts to define security governance have been enhanced by audit requirements for most public firms, and have been considered important enough to warrant separate sections of audit practices in formal programs such as COBIT, the Control Objectives for IT. Per von Solms:

Information Security Governance consists of the management commitment and leadership, organizational structures, user awareness and commitment, policies, procedures, processes, technologies and compliance enforcement mechanisms, all working together to ensure that the confidentiality, integrity, and availability (CIA) of the company’s electronic assets (data, information, software, hardware, people, etc.) are maintained at all times (von Solms, 2005b, p.444).

Tan, et al., (2004) view ISG from a process view and include decision making rights, input rights and participation, experience and decision making culture, strategic context, and accountability infrastructure in their definition. Most formal frameworks offered by professional organizations such as ISACA, the international standards organization OSI, or ITIL, the IT Infrastructure Library developed by the UK Office of Government Commerce, offer varying levels of detail about IT security and consider security governance to be a subset of overall IT governance. The most common best practice...
Methodologies include ISO 27001 (evolved from BS7799/ISO17799:2000), COBIT, and ITIL, although others are industry specific or common in the government sector. It is interesting to note that the ITIL framework was initiated in the late 1980s, but did not gain interest in the US until after the 2002 recession when governance became a priority. The ISO standards include guidance for certification efforts, an important element for service suppliers, outsourcers, or government contractors.

Each of these frameworks has evolved through several generations of development, and all are considered to be tools for organizations to begin their governance efforts and measure their progress against the full set of recommendations. Such methods have been severely criticized and labeled fallacious by some researchers in terms of their universal approaches to security mitigation (Siponen, 2003). Even with the presence of critics doubting the efficacy of the frameworks, many organizations choose to start with them and modify their processes and recommendations to their particular organizational context. The reality of dealing with security in the real world is such that no single methodology or framework will likely ever be a “one size fits all” solution, but rather starting points for ISM and security professionals to consider, applying what is most needed and relevant to their organization.

METHODOLOGY & SELECTED RESULTS

This paper is part of an ongoing longitudinal research project studying best practice and governance framework use in US organizations. Partial results from a survey that examined the adoption of IT governance methodologies, general IT best practices, and security governance are discussed here, reviewing where organizations were in their examination and adoption of frameworks in 2005. The second phase of the study explores issues and changes in light of economic challenges.

Invitations to respond to an electronic survey were sent in the fall of 2005 to a convenience sample of twenty northwest US organizations of mid to large size. The survey was also publicized in a well read IT electronic newsletter, and an additional 104 participants were self-recruited from this source. Survey respondents included organizations of all sizes, from small business (<100) to large (>5000), for profit, education, health care, and government agencies. It might be expected that excellent IT organizations would tend to be larger, but in seeking a realistic look at best practice, the rest of the population is equally interesting. Basic descriptive statistics reveal a fairly balanced sample based upon company size, industry, and geographic location, although self-selection clearly indicates respondents interested in the topic area. Academic literature and practitioner sources were searched to build questions relating to general and security best practice. No single source seemed to be all-inclusive for selecting established best practices, so those items appearing in multiple sources were chosen for the survey.

General IT Practices - Comparison to Top IT Organizations

The first stage of the study was to determine how well the survey respondent organizations compared to the best practice organizations in a survey of top 100 IT organizations as selected by CIO magazine. Table 1 lists the ten most utilized IT governance practices of the top organizations per the CIO study, and compares the author’s sample to those results. Numbers reflect the number of organizations who acknowledged that their organization utilized each practice.

<table>
<thead>
<tr>
<th>Top 10 Most Utilized IT Practices</th>
<th>CIO Top 100</th>
<th>Survey Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Regularly use project management methodologies</td>
<td>96</td>
<td>80</td>
</tr>
<tr>
<td>2. Conduct regular strategic planning meetings to achieve alignment</td>
<td>93</td>
<td>73</td>
</tr>
<tr>
<td>3. Conduct internal customer satisfaction surveys</td>
<td>86</td>
<td>58</td>
</tr>
<tr>
<td>4. Create and use performance metrics</td>
<td>84</td>
<td>58</td>
</tr>
<tr>
<td>5. Regularly use portfolio management or other project prioritization methodology</td>
<td>80</td>
<td>56</td>
</tr>
<tr>
<td>6. Perform financial audits</td>
<td>79</td>
<td>52</td>
</tr>
<tr>
<td>7. Use leadership development programs</td>
<td>79</td>
<td>49</td>
</tr>
<tr>
<td>8. Make the CIO a member of the corporate board or executive committee</td>
<td>76</td>
<td>27</td>
</tr>
<tr>
<td>9. Employ internal relationship managers/account executives to work with the business</td>
<td>75</td>
<td>57</td>
</tr>
<tr>
<td>10. Conduct post-implementation audits</td>
<td>74</td>
<td>42</td>
</tr>
</tbody>
</table>

Table 1. CIO’s 100 Excellent IT Organizations (2004) vs Survey of IT Organizations (2006), n = 124
The survey group scored lower for each of the most utilized IT practices, as might be expected for a cross-section sample of a broader population including non-profits and small organizations. The top two practices of planning to achieve alignment and project management compare reasonably well with the survey organizations, showing some success in the ongoing emphasis on these two topic areas.

**Formal Frameworks Explored**

The survey group was asked what their expectations were regarding best practice adoption, which best practice frameworks they had reviewed, and then which, if any, was ultimately adopted by their organization. The listed frameworks included some narrowly defined programs such as the Six Sigma and ISO 9000 quality processes, as well as broader IT service management models such as ITIL, (IT Infrastructure Library). This grouping was used to gauge the overall range of experience the group might have with formalized processes and frameworks. Table 2 lists the methodologies offered in the survey, with a brief description of their focus.

<table>
<thead>
<tr>
<th>Methodology</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BPR – Business Process Re-engineering</td>
<td>Method to improve processes &amp; operating efficiencies</td>
</tr>
<tr>
<td>CMM- Capability Maturity Model</td>
<td>Measurement of organization’s level of process capability maturity</td>
</tr>
<tr>
<td>COBIT – Control Objectives for IT</td>
<td>IT Governance audit guidelines from ISACA</td>
</tr>
<tr>
<td>ISO 9000</td>
<td>Standard for identification &amp; certification of quality processes</td>
</tr>
<tr>
<td>ISO 17799</td>
<td>Code of Practice for Information Security Management</td>
</tr>
<tr>
<td>ITIL – IT Infrastructure Library</td>
<td>Set of concepts and policies for managing IT service operations</td>
</tr>
<tr>
<td>Six Sigma</td>
<td>Management strategy targeting the identification &amp; removal of defects or errors in processes</td>
</tr>
<tr>
<td>TQM – Total Quality Management</td>
<td>Management approach centered on quality improvement</td>
</tr>
</tbody>
</table>

Table 2. Best practice and/or IT governance methodologies as defined in the survey

Many of the methods listed have evolved over time and continue to be improved or customized. The initial Capability Maturity Model, for example, has expanded into several specialty areas including the software engineering model, CMMI, and most recently, the Systems Security Engineering CMM, SSE-CMM (Carnegie Mellon, 2003). The only information security-specific methodology listed, ISO 17799, has been a work in process over time. Originating from the British BR7799 standard, this series was adopted and modified by the OSI resulting in ISO 17799. A new numbering scheme now includes this standard as ISO 27001, a specification for an information security management system. ISO 17799 has been globally recognized, including a validation analysis by Ma and Pearson (2005), which showed that eight of the ten security dimensions included are highly valid, with redundancy masking the results on the others. This study was an important effort to validate one of the most widely recognized information security frameworks.

ITIL is another British effort, a set of best practices and guidelines begun in the 1980s to specifically address IT service functions. A section of the framework addresses security management processes, and the general approach is one of defining objectives, activities, inputs, and outputs, but not how the processes should be implemented (Weill, 2004). This latter feature allows organizations to implement the recommendations in the manner most consistent with their operations. The Control Objectives for IT (COBIT) was developed by the Information Systems Audit & Control Association, as a set of audit guidelines and IT governance measures, and is widely used by internal audit groups to measure IT effectiveness. They have recently released The Business Model for Information Security, (2009) which they hope will provide a view of information security program activities within the larger context of the enterprise.

The initial expectations of survey respondent regarding best practice adoption are shown in Chart 1, where they clearly identify increased efficiencies and process improvement as the top goals by 70% or more participants, with response to regulatory compliance noted by more than half.

Chart 2 shows the various frameworks reviewed by survey respondents, along with those either adopted or declined. Approximately 25% of respondents who acknowledged they used best practices did not adopt or consider any of the frameworks listed in the survey. This group of respondents listed other methods such as COBIT as proposed by their internal
audit staff, or specialized programs such as Air Force Instruction Set, Toyota TPM, and NIST (National Institute of Standards & Technology) Guidelines.

Chart 1. Expected Benefits of BP Adoption

Approximately 23% of total respondents used no best practice programs either at the organization level, or in IT. Of those adopting a framework, 46% had no monitoring or measurement system in place to track results. When considering a typical five-level maturity scale of “initial, repeatable, defined, managed, optimizing,” (CMM User Portal) one might conclude then, that this particular sample group was immature in terms of their use of formal methodologies, in that they had not yet evolved to the level of governance whereby assessment is in place to ensure processes are managed and measureable.

Information Security Management Practices

To gauge what level of information security management practice was implemented by survey respondents, questions were developed relating to security practices in the ten areas of the Common Body of Knowledge (CBK) on security as defined by the International Information Systems Security Certification Consortium, Inc. (ISC²). This organization develops and supports globally recognized security certifications, including the recently added ISM-oriented ISSMP (Information Systems Security Management Professional), the general CISSP (Certified Information Systems Security Professional), and the operations-oriented SSCP (Systems Security Certified Practitioner). The CBK offers a logical way to organize areas of security risk, with many sources available to help organizations achieve threat mitigation.

Table 3. Degree to which each of the CBK areas was adopted by the respondents

As Table 3 reflects, survey respondents admit to being at varying levels of maturity in terms of process adoption in these ten areas. Respondent organizations indicate they have obtained the greatest degree of best practice adoption in that of physical
security, with network architecture and management practices close behind, and the lowest level of best practice adoption in their use of cryptography to protect their data resources.

Relating more specifically to ISM goals, respondents were asked which security best practices listed had been adopted by their organization, as well as for which categories they had formal strategies. Of organizations who have adopted general IT best practices, less than half of the respondents had progressed in their maturity level to adopt specific ISM best practices. Chart 3 reflects having full-time security staff as the most often employed practice, and incident reporting to be the least adopted. The latter is consistent with other studies that indicate many organizations are reluctant to report security incidents, for fear of a negative response from customers and the market. This is likely to continue to be true for other than legally mandated reporting requirements.

Organizational efforts at developing and implementing formal strategies for key security components are shown in Chart 4, reflecting that the most commonly implemented strategies are for business continuity and disaster recovery. While respondents indicated in Table 3 that security best practice was in place for the organization’s network architecture, Chart 4 reveals they are less likely to have a formal strategy in place for a well defined security architecture. It is disappointing to note that less than 70% of respondents report that they have a formal information security strategy in place.

Organizations report a variety of benefits from best practice adoption, including better all around information security and privacy for approximately 58% of those best practice adopters. Responses in this category, shown in Chart 5, may also reflect that not all organizations are measuring the benefits of their best practice effort.
CONCLUSION & FUTURE RESEARCH

This brief summary of survey results from research in progress addresses the current shortfall in the security literature regarding the adoption and implementation of frameworks and methodologies in ISM practices and security governance. While the survey respondent population was relatively small, a cross-section of respondents reflects a growing interest in best practice adoption leading to information security governance, as well as frameworks that can help organizations achieve desired results faster. Frameworks are of interest to organizations who expect the adoption of proven processes to enhance operational efficiency, help achieve regulatory compliance, and reduce the time and effort involved with implementing improvement programs. Some of the results clearly suggest that organizations in the survey sample are slowly adopting best practices in the ISM area.

Many unanswered questions are left for future research. The second phase of this study includes returning to the survey organizations to see where they are today in their implementation, and semi-structured interviews with selected survey respondents to explore some of the more interesting outcomes and missing explanations. These interviews will identify changes in the organization’s use of best practice methodologies in general, and security best practices in particular, since the date of the original survey. They will also explore organization experiences in adopting or modifying the frameworks to better align with organizational context and risk profile, and identify key areas where frameworks are most likely to be modified to fit organizational risk.

REFERENCES