Integration of COBIT, Balanced Scorecard and SSE-CMM as a strategic Information Security Management (ISM) framework

Suchit Ahuja[1], James E. Goldman[1]

[1] Purdue University, Department of Computer & Information Technology, West Lafayette, IN 47907, USA

Abstract

The purpose of this study is to explore the integrated use of Control Objectives for Information Technology (COBIT) and Balanced Scorecard (BSC) frameworks for strategic information security management (ISM). The goal is to investigate the strengths, weaknesses, implementation techniques, and potential benefits of such an integrated framework. This integration is achieved by "bridging" the gaps or mitigating the weaknesses that are recognized within one framework, using the methodology prescribed by the second framework. Thus, integration of COBIT and BSC can provide a more comprehensive mechanism for strategic information security management (ISM) – one that is fully aligned with business, IT and information security strategies. The use of Systems Security Engineering Capability Maturity Model (SSE-CMM) as a tool for performance measurement and evaluation can ensure the adoption of a continuous improvement approach for successful sustainability of this comprehensive framework. There are some instances of similar studies conducted previously:

- metrics based security assessment [1] using ISO 27001 and SSE-CMM
- mapping of processes for effective integration of COBIT and SEI-CMM [2]
- mapping of COBIT with ITIL and ISO 27002 [3] for effective management and alignment of IT with business

The factor that differentiates this research study from the previous ones is that none of the previous studies integrated BSC, COBIT and SSE-CMM, to formulate a comprehensive framework for strategic ISM that is aligned with business, IT and information security strategies. Therefore, a valid opportunity to conduct this research study exists.

Keywords: Business/IT Alignment, Business/IT/Information Security Alignment, Balanced Scorecard, Strategic Information Security, Control Objectives for Information Technology (COBIT), Systems Security Engineering Capability Maturity Model (SSE-CMM)

1 Introduction

Threats to security of business information, information-based assets, intellectual property, and privacy of personal information are increasing. In order to counter these threats, information security management (ISM) is gaining increasing importance within organizations, becoming almost imperative as security threats continue to escalate. According to a study by McAfee [4], data theft and breaches from cybercrime may have cost businesses as much as $1 trillion globally in lost intellectual property and expenditures for repairing the damage in 2008. Regulatory compliance requirements, loss of revenue, loss of stakeholder confidence, and loss to brand and reputation are drivers for investment in the implementation of such ISM frameworks (like ISO 27001, ISO 27002, COBIT, etc.) as indicated by Ernst & Young's (E&Y) Global Information Security Survey in 2008 [5]. This indicates that information security frameworks are used only as a partial solution in order to protect information and to secure assets, without integrating them with the business strategy. E&Y [5] also further validates this by reporting that only 18% of the organizations surveyed had information security strategy as an integrated part of their overall business strategy. This lack of alignment between business, IT and information security strategies is also highlighted by IT Governance Global Status Report [6], which shows that between 2005 and 2008, the number of organizations reporting disconnect between IT strategy and business strategy, increased by almost 30%. In order to mitigate risks caused by lack of alignment with respect to ISM, a holistic and comprehensive framework must be developed such that it not only addresses technical aspects of security but also takes into account business alignment, IT governance, and measurement and evaluation [7]. As organizations adopt ISM frameworks more aggressively, governance, risk management, and compliance (GRC) spending exceeded $32B for 2008, up 7.4% from 2007 [9]. The use of one ISM framework is inadequate to address ISM requirements comprehensively, hence a large number of organizations use an internally developed framework to address their ISM requirements, by integrating two or more recognized security frameworks or mechanisms [6].

The strategic integration of these frameworks is often challenging for the organization. Nevertheless, organizations that successfully implement an ISM framework via a combination of standards and best practices (for strategic ISM) may gain considerable value and benefits. This view is supported by studies showing the integration of ISO, ITIL and COBIT [8]; ISO and SSE-CMM for metrics based security assessment [1]; mapping of processes for effective integration of COBIT and SEI-CMM [2]; and COBIT with ITIL and ISO 27002 [3] for effective alignment of IT with business.

Similarly, this study proposes the integrated use of Control Objectives for Information Technology (COBIT) and Balanced Scorecard (BSC) frameworks for strategic ISM. The goal is to investigate the strengths, weaknesses, implementation techniques, and potential benefits of such an integrated framework. Such an integrated framework bridges the gaps or mitigates the weaknesses that are recognized within one framework, using the methodology prescribed by the second framework. Thus, the integration of COBIT and BSC can provide a more comprehensive mechanism for strategic ISM – one that is fully aligned with business, IT and information security

strategies. It is also important to measure and evaluate the performance of the integrated "strategic ISM framework" using a standards based model, like the Systems Security Engineering Capability Maturity Model (SSE-CMM). This will enable evaluation of the effectiveness of the framework and enhance the ISM process by adoption of a continuous improvement approach. This study aims to design a comprehensive ISM framework while trying to add value to previously established principles.

COBIT is an international open standard that defines requirements for the control and security of sensitive data and provides a reference framework [35]. COBIT has gained significant popularity as an IT governance mechanism in recent years and according to PriceWaterhouseCoopers [10] between 2003 and 2006, the awareness of COBIT has tripled amongst the general IT population, while awareness in the general population of the existence of COBIT has increased by 50 percent. On the other hand, the total usage of BSC has also doubled between 1993 and 2006, with about 57% of global companies working with the BSC in one or more functions [11]. SSE-CMM is internationally recognized and a widely accepted model for measurement and evaluation of security processes and controls across the organization [12]. The integrated use of the three suggested frameworks can potentially prove to be highly effective for strategic ISM.

2 Background

COBIT is an IT governance framework and supporting toolset that allows managers to bridge the gap between control requirements, technical issues and business risks [2]. Balanced Scorecard by definition is a performance management system that enables businesses, business units and functional business areas to drive strategies based on goal definitions, measurement, and targets [24][25]. SSE-CMM is a widely accepted security 'process reference' model that is used across various business units within an organization due to its "methodology neutral" approach [1][12].

2.1 Strengths & Weaknesses of COBIT from an ISM perspective

The IT Governance Institute reports that COBIT enables clear policy development and good practice for IT control throughout organizations. COBIT emphasizes regulatory compliance, helps organizations in increasing value attained from IT, and enables business/IT alignment [14][15][16]. Interestingly, this perspective does not provide details about how COBIT can support a business-IT-information security alignment strategy or how IT security controls can be implemented. Thus, by default due to its popularity as a governance tool, COBIT is often categorized as a tool for management purposes. This categorization of COBIT focuses only on the management aspects (like decision-making) and ignores the process-level controls that the COBIT framework is built on. There is some evidence of using COBIT as an alignment tool but the alignment started only at the prescribed COBIT process levels instead of using an alignment methodology that cascaded from the organizational-level mission to the information security controls [17]. Hence, the solution remained incomplete in terms of business-IT-security alignment.

COBIT originated from an attempt to improve auditing and this makes it a perfect frame of reference for the internal control of IT, guaranteeing performance measurement, value creation and risk management [18]. COBIT has also become a

de-facto standard especially in financial organizations [19] thereby making it universally applicable. There are several examples of using COBIT and SEI-CMM in order to measure the maturity of processes within an organization [2][3][8][20]. It is detailed in its description of process-level controls. COBIT has important business value, including increased compliance, corporate risk reduction, good accountability, and proves to be a useful tool to establish a baseline for process maturity [20].

In contrast, from an ISM perspective, COBIT has some recognized weaknesses. Although IT governance is considered an enabler for business/IT alignment, COBIT lacks in the establishment of responsibilities and a methodological alignment with the business strategy – especially when COBIT processes are used for enabling ISM [18][21][23]. This is by far the biggest weakness that must be mitigated by using another framework; or else the purpose of using COBIT would be defeated if the recommended processes (over security controls) are not fully aligned with business strategy. The following weaknesses have also been reported by [22][23]:

- Incongruence exists within COBIT like control objectives not being effectively mapped to process areas and not aligned with business requirements.
- Each COBIT domain specifies its own maturity measurement model, based on process areas within that domain. These maturity levels are not arranged in a way such that the aggregation from separate domain-level metrics can be aggregated into a comprehensive maturity level for the organization or business unit.
- COBIT does not aid efficient data collection and it does not provide guidelines or options for partial implementation.
- The analysis of a COBIT implementation is difficult to achieve and cannot be automated. The result of a COBIT supported IT governance maturity assessment might vary from one time to another depending on several factors like the time when an analysis was conducted, the person who conducts the analysis, the processes that are being analyzed, etc.

As COBIT controls are exercised at the domain and process level, it is often difficult to adapt to specific areas within an organization and is therefore resisted in terms of implementation [19]. COBIT for information security governance is not very detailed in terms of 'how' controls or best practices processes can be implemented [19][20].

2.2 Strengths & Weaknesses of Balanced Scorecard

The balanced scorecard usually consists of four specific domains as listed below:

1. the business contribution perspective capturing the business value created from various investments (in the context of this research study, security investments)
2. the user perspective representing the user evaluation
3. the operational excellence perspective evaluating the IT processes employed to develop and deliver applications
4. the future perspective representing the human and technology resources needed by information security to deliver its services over time

The domains can be tweaked to fit the information security strategy [26]. In order to achieve business-IT-security alignment, it is important to use the cascading BSC approach. "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)" [27]. The cascading balanced scorecard approach (between business and IT) can be successfully used as a strategic management tool [24][27][28][29]. In [25], figures 9, 11 and 14 clearly show

a graphical representation of this cascading BSC approach. The organizational alignment should be clearly visible through strategy, using the strategy map, performance measures and targets, and initiatives. Some weaknesses exist while trying to use only a cascading BSC approach for ISM. The BSC approach to effective strategic management is often seen as subjective and difficult to implement. According to [30], the use of BSC can cause disagreement and tension between top and middle management regarding the appropriateness of specific aspects of the BSC as a communication, control and evaluation mechanism. This is one of the most significant drawbacks of using BSC and in order to minimize risks, it is important to use a governance mechanism that sets the priority for evaluation parameters (as a guideline for executive management) within the context of the BSC approach. There is disagreement about how the balanced scorecard can link strategy to operational metrics, which managers can understand and influence [24]. It is also difficult to establish traceability from the business-level down to the information security-level without using a governance framework to guide information criticality and set the appropriate priority, which can in turn guide the information security strategy.
The above discussion proves that BSC is a multi-purpose tool that can be used as a performance management system [25], IT governance mechanism [32] and as a strategic alignment framework [24], but when it is used as a standalone mechanism for comprehensive alignment of business/IT/security strategies, its weaknesses and gaps are exposed. On the contrary, COBIT is highly effective when used as a standalone mechanism for IT governance, but is lacking when assessed from a business/IT alignment perspective.

2.3 Measurement of information security process maturity via SSE-CMM

It is difficult to measure security controls and security processes, both qualitatively and quantitatively [33][34]. In order to counter a vast range of potential vulnerabilities and a huge scale of threats, a strategic approach to measurement of the maturity of security processes and controls is required [9]. 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" [1]. The internal maturity model within COBIT is narrow in scope and covers only individual COBIT domains. There is no provision for aggregation of metrics across domains in order to implement a comprehensive, organization-wide maturity model [22].SSE-CMM maturity model facilitates synergy between system life cycle phases, increases efficiency, reduces wastage, and results in more secure solutions with greater assurance and lower costs [1][9]. It is a widely accepted security 'process reference' model that is used across various business units within an organization due to its "methodology neutral" approach [1][33]. In order to provide meaningful ISM process maturity reports to the business and to build a framework that enables a continuous improvement approach, the use of SSE-CMM as a measurement and performance evaluation tool is required.

3 Methodology

In order to integrate these existing frameworks it is important to understand how they work individually and then conduct a detailed study of how they can be integrated. It is imperative to study where the gaps may exist and where synergy can be obtained

during the integration process. Hence, the methodology used consists of the following steps: 1) Review of existing literature, 2) Gap analysis of COBIT and BSC frameworks, and 3) Mitigation of gaps based on previous research and some value added from current efforts.
The goal is to establish clear traceability within such an integrated framework using a top-down approach from business-level to operational security level. In order to achieve this, it is critical to ensure that the output (in terms of metrics, KPIs, targets, and initiatives) of one framework is aligned perfectly with the input (in terms of objectives, KGIs, mission, etc.) of the other framework, thereby establishing a robust input-process-output methodology.

4 COBIT – BSC Gap Analysis

In order to design an integrated "strategic ISM framework" that uses COBIT, BSC, and SSE-CMM, the gaps that exist within each individual framework must be studied. In order to highlight these gaps, these frameworks must be analyzed separately. APPENDIX A below shows the various components of the COBIT & BSC frameworks when used individually, following a top-down approach starting from business information and going down to ISM processes and controls. The two scenarios in APPENDIX A highlight the gaps of both frameworks.
Table 1 lists the gaps and weaknesses and provides potential mitigation solutions.

Table 1: Weaknesses in BSC & COBIT - and potential mitigation solutions

#	Weaknesses / Risks / Gaps	Mitigation Mechanism
1	**COBIT**	
1.1	Lack of alignment of COBIT process areas with business strategy	Use a cascading balanced scorecard approach to align business strategy with information security strategy that can be used as input to COBIT process areas [26]
1.2	A vast amount of metrics that can be used to assess the maturity of IT governance. These are however not arranged in a way such that the aggregation from separate metrics into a comprehensive maturity level is supported	Use metrics from cascading BSC and Key Performance Indicators (KPI), Key Goal Indicators (KGI) and Critical Success Factors (CSF) to aggregate the metrics towards a comprehensive maturity level; using maturity levels prescribed by SSE-CMM as a guideline [20] [3]
1.3	A maturity model that is mainly a stand-alone analysis tool that provides only a very shallow analysis of the situation.	Use SSE-CMM mapping to COBIT areas, a maturity model can be developed. Previous research has mapped COBIT to SEI-CMM [2]
1.4	Audit and Information Security reporting gaps can lead to lack of information flow between upper management and implementation teams.	Using a cascading balanced scorecard approach would establish an information security reporting mechanism via KPIs, KGIs and CSFs while measuring maturity via SSE-CMM [26] [20]
2	**Balanced Scorecard**	
2.1	Can cause disagreement and tension between top and middle management regarding the appropriateness of specific aspects of the BSC as a communication,	The use of COBIT as a governance tool for business, IT and information security management strategies. The use of COBIT Information Classification / Criteria, with clear prioritization can mitigate risks arising

	control and evaluation mechanism.	from conflicts [8]
2.2	Terminates at the "Initiatives" level without indicating what processes need to be implemented or "how" the initiatives must be implemented	Create a mapping between COBIT processes and BSC initiatives
2.3	Lack of traceability from business to information security level. Additional tools or frameworks are required in order to ensure that a process lifecycle is established for the management of initiatives	Use of COBIT control processes over appropriate process areas that are related to information security management
2.4	Audit and Information Security reporting gaps can lead to lack of information flow between upper management and implementation teams.	Using a cascading balanced scorecard approach would establish an information security reporting mechanism via KPIs, KGIs and CSFs while measuring maturity via SSE-CMM [26][20]

5 Mitigation of Gaps

Using an integrated approach that combines BSC, COBIT and SSE-CMM, the gaps identified in Table 1 can be addressed and mitigated. APPENDIX B below provides a detailed view of the tools and processes that can be used to achieve this mitigation. The use of a top-down framework to display the mitigation of gaps is used, in order to design an integrated framework and to maintain an appropriate process flow for ISM.

5.1 Information / IT Governance Gap (#2.1)

The use of COBIT Information Criteria can result in effective classification of information, based on a clear set of criteria as defined by the organization, leading to lower risks and avoidance of conflicts between executive management (pertaining to information criticality and prioritization). These criteria include the following: Effectiveness (EFT), Efficiency (EF), Confidentiality (CF), Integrity (I), Availability (A), Compliance (C), and Reliability (R).

According to European University Information Systems (EUNIS), COBIT Information Criteria overlap largely with the audit criteria of Netherlands' Professional Association of Accountants NIVRA-53 [36], which provides standards for the auditor's statement relating to electronic data processing. Thus, using COBIT Information Criteria can help in the classification of information directly for audit purposes and establish ease of top-down traceability. The COBIT Information Criteria matrix is also similar to the Information Criticality Matrix (ICM) that is part of the Infosec Assessment Methodology (IAM) developed by the National Security Agency (NSA). ICM enables the classification of information based on organizational requirements and is a widely accepted mechanism. The ICM uses a standard C-I-A (confidentiality, integrity, availability) model to classify information, while COBIT uses broader classification criteria, thereby providing flexibility to the organization, which can result in effective information governance (Figure 1). This concept can be mapped directly to the COBIT process area of "Plan & Organize", recommending that an organization must "Define the Information Architecture (PO2)" and consists of PO2.1 - Enterprise Information Architecture Model, PO2.2 - Enterprise Data Dictionary and Data Syntax Rules, PO2.3 - Data Classification Scheme, and PO2.4 - Integrity Management. To that end, using COBIT Information Criteria provides an

appropriate platform for developing clear high-level priority for information protection as a guidance baseline for COBIT control processes. This enables alignment of business requirements directly with information security controls, while simplifying the implementation of information security tools and processes.

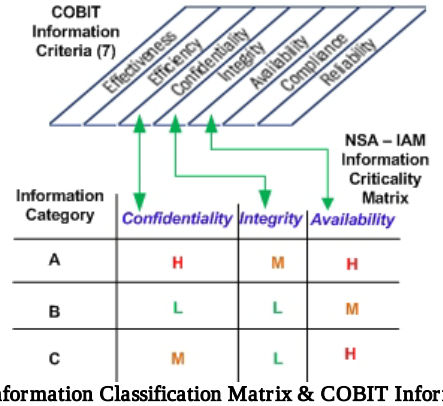


Figure 1: Information Classification Matrix & COBIT Information Criteria

5.2 Business Alignment Gap (#1.1)

The COBIT process area "Plan & Organize (PO1) requires the establishment of a strategic IT plan. Nevertheless, COBIT does not provide any tool or mechanism to enable the development or deployment of a strategic IT plan. The use of a cascading BSC approach is required to address this gap (# 1.1) as shown in Figure 2 below. The use of a cascading BSC establishes alignment between the business strategy (based on business processes and information), IT strategy and information security strategy, thereby enabling the extrapolation of a unified strategy across the organization from the executive management to the operational level. In [25], figures 9, 11 and 14 clearly show a graphical representation of this cascading BSC approach. 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).

5.4 InfoSec Audit and Up-Reporting Gaps (#1.2, 2.2)

Using the methodologies described in [1], [2], and [3], SSE-CMM process areas must be mapped to appropriate COBIT process controls. The resulting business metrics can be reported to upper management via the KPI/KGI cascade and the resulting information security metrics can be reported via the COBIT process area of "Measure and Evaluate (ME)". Figure 3 below shows an example of the metric reporting processes. The goal is to ensure continuous reporting of security metrics (to executive management) from both business and operational level security processes. In order to achieve this, it is important to establish traceability between the metrics that are established as part of the business, IT, and information security strategies. Metrics and targets established at the BSC level can be used a baseline for comparison. The Key Goal Indicators (KGIs) of the business and the initiatives from the cascading BSC must be synchronized. On the other hand, the process goals within COBIT must be clearly defined and mapped to the BSC initiatives. The KGIs and COBIT goals drive

the Key Performance Indicators (KPIs) of the information security BSC and the COBIT process area of "measure & Evaluate" respectively. These in turn are used to measure the performance of the COBIT control processes that monitor the operational security controls. This type of a reporting mechanism supports the meaningful reporting of security audit data directly to the business level, thereby contributing towards enhancing the conversion effectiveness of operational security controls.

Figure 2: COBIT - Cascading BSC Mapping

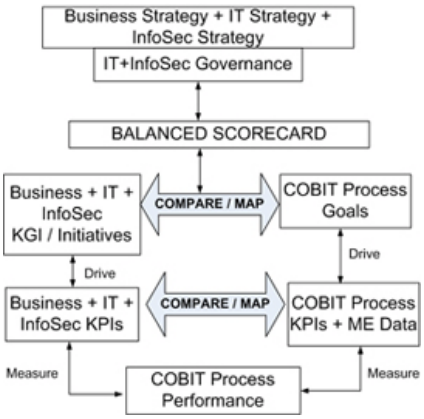


Figure 3: Cascading KPIs & KGIs for mitigation of Audit/Up-Reporting Gaps

5.5 Maturity Measurement Gaps (#1.3, 1.4, 2.3, 2.4)

The maturity levels defined in COBIT process areas are very generic. The definition and requirement to achieve a particular maturity level is dependent on organizational expectations and can be easily misinterpreted. Therefore, a standardized mechanism to measure process-level maturity for information security is required. This can be achieved by using the maturity levels defined in SSE-CMM. Using the methodologies described in [1], [2], [3], [22] and [37], SSE-CMM maturity level definitions must be mapped to appropriate COBIT process area maturity levels, thereby providing a measureable and traceable mechanism to measure information security process maturity. This will facilitate the establishment of a "continuous improvement" approach to information security. The basic idea is to create a mapping between COBIT domains and SSE-CMM process areas (PAs) such that the organization can use this to streamline the common functions and to align processes in order to achieve

an efficient ISM approach. SEI-CMM (which is primarily used to measure software development "process maturity") has been used mapped to COBIT domains in [2]. A potential solution (in the context of this research study) is to use a similar methodology and replace SEI-CMM Process Areas with SSE-CMM Process Areas. In order to meet the length limitations and for simplification purposes, only a summary of the mapping structure is shown in Table 2 below. The SSE-CMM process areas (PA) and base practices (BP) are directly referenced from [12]. The focus was on the "security" based COBIT domains and hence DS5-Ensure Systems Security was expanded, while only a high-level mapping of the other three domains is shown.

Table 2: Summary of SSE-CMM and COBIT mapping

COBIT Processes	SSE-CMM Process Areas (PA) & Base Practices (BP) High Level Correlation	CMM Levels
Plan and Organize (PO)		
PO1 – PO 11	Managed by Business/IT Alignment	N/A
Acquire and Implement (AI)		
AI 1 – AI 6	Managed by organizational processes	N/A
Deliver and Support (DS)		
DS1 Define & Manage service levels	PA 01(BP: 1-4)	3 - 5
DS2 Manage third party services	PA 12 – PA 22	1 - 5
DS3 Manage performance & capacity	PA 12 – PA 22	1 - 5
DS4 Ensure continuous service	PA 12 – PA 22	3 - 5
DS5 Ensure systems security		
5.1 Mgmt. of IT Security	PA 01(1-4), PA 02(1-6), PA 03(1-6), PA 04(1-6), PA 05(1-5)	3 - 5
5.2 IT Security Plan	PA 06(1-5), PA 10(1-7)	1 - 3
5.3 Identity Mgmt.	PA 01 – PA 11	1 - 3
5.4 User Account Mgmt.	PA 01 – PA 11	1 - 3
5.5 Testing, surveillance, monitoring	PA 06(1-5), PA 08(1-7)	3 - 5
5.6 Security incident definition	PA 02 (1-6), PA 03(1-6)	3 - 5
5.7 Protection of security technology	PA 07(1-4), PA 08(1-7)	3 - 5
5.8 Cryptographic key mgmt.	PA 01 – PA 11	1 - 3
5.9 Prevention, detection & correction	PA 03(1-6), PA 07(1-4), PA 08(1-7)	3 - 5
5.10 Network Security	PA 01 – PA 11	1 - 3
DS6 Identify & allocate costs	PA 12 – PA 22	N/A
DS7 Educate & train users	PA 01(3), PA 09(5-6), PA 10(2)	3 - 5
DS8 Assist & advise customers	PA 10(1-7)	3 - 5
DS9 Manage configuration	PA 01(1-4), PA 07(1-4)	3 - 5
DS10 Manage incidents	PA 03(1-6), PA 07(1-4), PA 08(1-7)	3 - 5
DS11 Manage Data	PA 03(1-6), PA 07(1-4), PA 08(1-7)	3 - 5
DS12 Manage facilities	PA 12 – PA 22	N/A
DS13 Manage Operations	PA 12 – PA 22	N/A
Monitor and Evaluate (ME)		
ME1 Monitor & Evaluate IT performance	PA 11(1-5)	3 - 5
ME2 Assess internal control adequacy	PA 11(1-5), PA 8(1-7)	3 - 5
ME3 Ensure regulatory compliance	PA 10(2), PA 06(1-5), PA 11(1-5)	3 - 5
ME4 Provide IT Governance	PA 11(1-5), PA 03(1-6) + strategic alignment	4 - 5

6 Limitations

The integration of COBIT, BSC and SSE-CMM for the purpose of strategic ISM is conceptual at this stage. COBIT is a resource intensive framework that requires training and takes considerable time to implement and analyze [14][22]. It would be difficult for an organization to integrate it within its existent ISM processes and alignment frameworks solely to provide results for this research study. Hence, this study is not based on results from an implementation. Although the ValIT framework is seen as more tightly integrated with COBIT, it was not considered for the purposes of this research study due to its focus on information security from the perspective of investments, while the focus of this paper is Business/IT/Information Security alignment. The extensive use of BSC in academic research and industry implementation provides quality literature and credibility. ValIT is comparatively new and does not possess a significantly large publication base.

7 Conclusion

In order to develop a comprehensive "strategic information security management" framework, it is critical to consider the alignment of the business, IT and information security strategies. It is also important to consider that the development of such a framework must take into account organizational entities such as applications, information, infrastructure and people. The success of the information security framework is dependent on the establishment of traceability between policy, process, people, procedures and technology. The success of the framework can be measured in terms of conversion effectiveness of the business goals into IT goals and IT goals into information security goals, thereby proving that the strategies are aligned and that the success of execution (of those strategies) is quantitatively measurable. The use of a gap analysis and gap mitigation methodology, along with the input-process-output functionality, enables clear traceability and supports implementation. Using the integration of COBIT, BSC and SSE-CMM frameworks, the development of such a conceptual framework for strategic ISM is achievable.

References

[1] Goldman, J.E., Christie, V.R. (2004). Metrics based Security Assessment. In Information Security and Ethics: Social and Organizational (pp 261-287). IRM Press.

[2] COBIT Mapping: Mapping SEI's CMM for Software with COBIT 4.0. (2007). *IT Governance Institute*. http://www.isaca.org/Template.cfm?Section=COBIT_Mapping1&Template=/ContentManagement/ContentDisplay.cfm&ContentID=27170

[3] IT Governance Institute. (2008). Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit. http://www.isaca.org/Template.cfm?Section=COBIT_Mapping1&Template=/ContentManagement/ContentDisplay.cfm&ContentID=45932

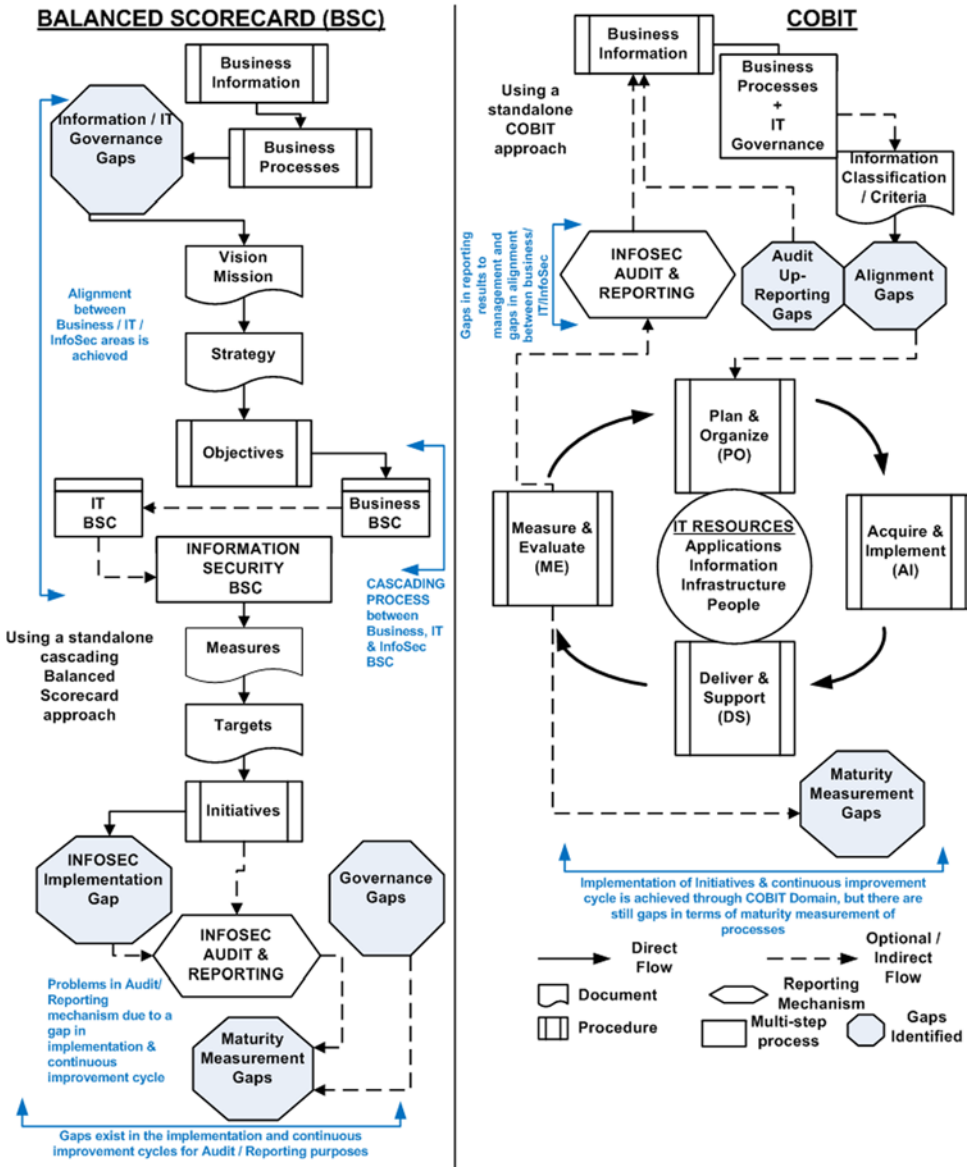
[4] McAfee. (2009). http://news.zdnet.com/2100-9595_22-264762.html

[5] Ernst & Young. (2008). Global Information Security Survey. http://www.ey.com/Global/assets.nsf/UK/Global_Information_Security_Survey_2008/$file/EY_Global_Information_Security_Survey_2008.pdf

[6] IT Governance Global Status Report. (2008). IT Governance Institute. http://www.itgi.org/AMTemplate.cfm?Section=ITGI_Research_Publications&Template=/ContentManagement/ContentDisplay.cfm&ContentID=39735
[7] Von Solms, B. (2001). Corporate Governance and Information Security. *Computers & Security*, 20(3), pp. 215-218.
[8] Turner, M.J., Oltsik, J., McKnight, J. (2008). ISO, ITIL and COBIT triple play fosters optimal security management execution. *SC Magazine Awards 2009 - USA*. http://www.scmagazineus.com/ISO-ITIL-and-COBIT-triple-play-fosters-optimal-security-management-execution/article/108620/
[9] AMR Research. (2008). The Governance, Risk Management, and Compliance Spending Report. http://www.amrresearch.com/
[10] PriceWaterhouseCoopers. (2006). IT governance survey 2006. http://www.pwc.com/Extweb/pwcpublications.nsf/docid/D3E2997D370F3C648025713300511A01
[11] Rigby, D. (2009). Management Tools and Trends 2007. Bain & Company Publication. http://www.bain.com/management_tools/tools_balanced.asp?groupCode=2
[12] SSE-CMM.org. (2009). How secure is SSE-CMM? Retrieved on 03/05/2009 from http://www.secure-software-engineering.com/2008/02/19/how-secure-is-sse-cmm/
[13] IT Governance Institute. (2007). *COBIT 4.1Handbook*. http://ww.itgi.org
[14] Ridley, G., et al. (2004). COBIT and its utilization: A framework from the literature. *Proceedings of the 37th Hawaii International Conference on System Sciences.*
[15] Larsen, H. M., Pedersen, K. M., and Viborg Andersen, V. K. (2006). IT Governance – Reviewing 17 IT Governance Tools and Analysing the Case of Novozymes A/S. P*roceedings of the 39th Hawaii International Conference on System Sciences,* 2006
[16] Debraceny, 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
[17] Haes, S. & Grembergen, W. (2005). IT Governance Structures, Processes and Relational Mechanisms: Achieving IT/Business Alignment in a Major Belgian Financial Group. HICSS pp. 237b, *Proceedings of the 38th Annual Hawaii International Conference on System Sciences* (HICSS'05) - Track 8, 2005
[18] Rouyet-Ruiz, J. (2008). COBIT as a Tool for IT Governance: between Auditing and IT Governance. 2008. *The European Journal for the Informatics Professional*. Vol. IX, issue No. 1, February 2008.
[19] Curtis, M.B., and Wu, F.H. (2000). The components of a comprehensive framework of internal control. *The CPA Journal*, 70(3): 64-66.
[20] Grembergen, W., Haes, S. (2005). *COBIT's Management Guidelines Revisited: The KGIs/KPIs Cascade*. IT Governance Institute Publication, Volume 6.
[21] Ernest, M. (2007). Adding value to the IT organization with the Component Business Model. IBM Systems Journal, 46(3): 387-389.
[22] Simonsson, M., Johnson, P. and Wijkström, H. (2007). Model-based IT Governance Maturity Assessments with COBIT. *KTH Royal Institute of Technology - Publications and Reports of School of Electrical Engineering.*

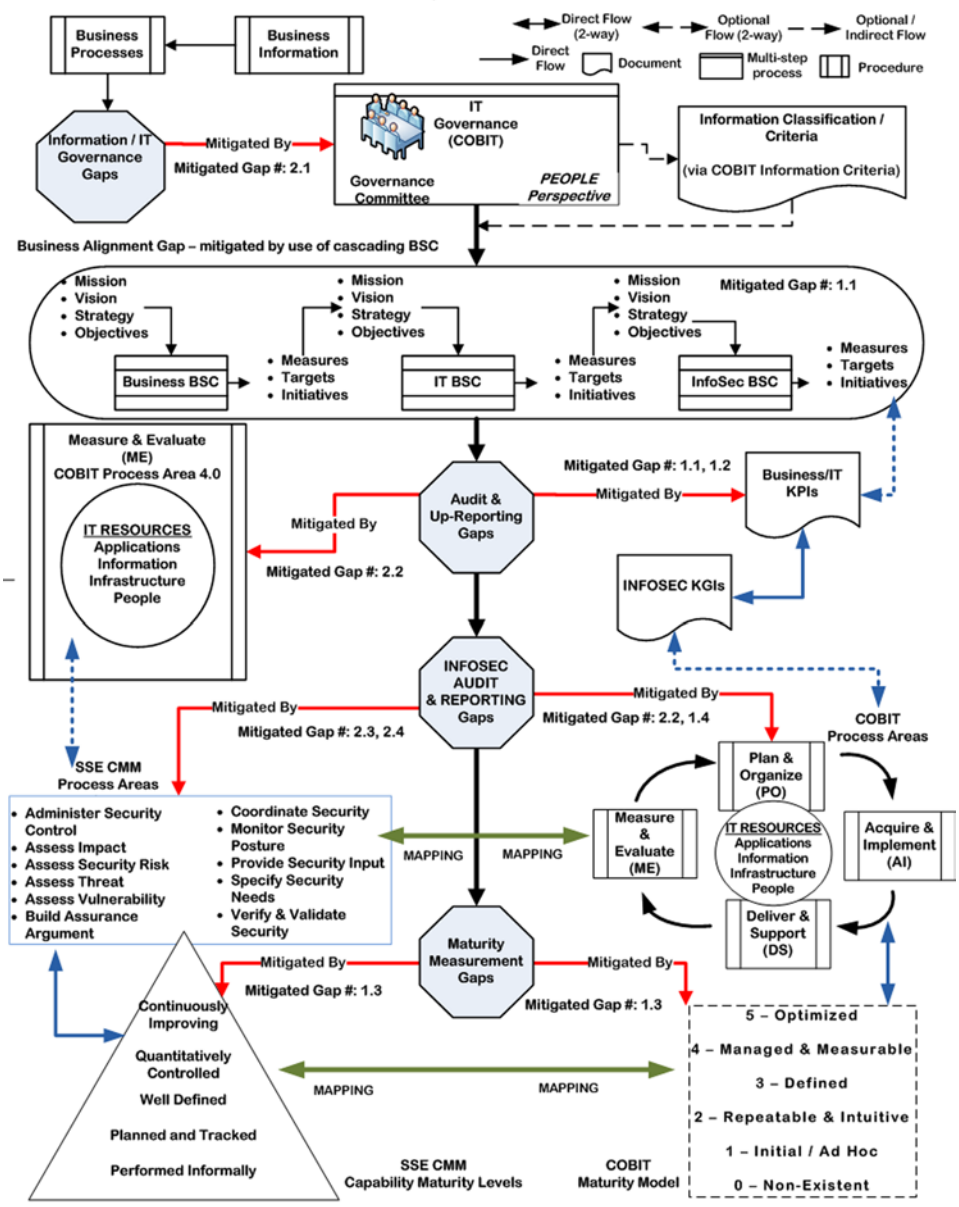
http://www.ee.kth.se/php/modules/publications/reports/2007/IR-EE-ICS_2007_026.pdf
[23] Ritchie, W. (2007). Old School CIOs versus COBIT - Avoiding COBIT is avoiding the emerging standards of IT accountability. *CIO Digest – Strategies and Analysis from Symantec.* http://www.symantec.com/business/theme.jsp?themeid=ciodigest
[24] Kaplan, R. S. (2005). The Balanced Scorecard: Measures that Drive Performance. Harvard business review, 83(7), 172-173.
[25] Rohm, H., Halbach, L. (August 2005). Developing and Using Balanced Scorecard Performance Systems. *The Balanced Scorecard Institute*.
[26] Microsoft (2007). Balanced Scorecard for Information Security Introduction. *Microsoft TechNet – Security TechCenter.* http://technet.microsoft.com/en-us/library/bb821240.aspx
[27] The Balanced Scorecard Institute. (2008). http://www.balancedscorecard.org/
[28] Ahn, H. (2001). Applying the Balanced Scorecard Concept: An Experience Report. *Long Range Planning*. 34(4), pp. 441-461.
[29] Kaplan, R. S. (2005). The Balanced Scorecard: Measures that Drive Performance. Harvard business review, 83(7), 172-173.
[30] Malina, A.M. and Selto, F. H. (2001). Communicating and Controlling Strategy: An Empirical Study of the Effectiveness of the Balanced Scorecard Approach. *Journal of management accounting research*. http://ssrn.com/abstract=278939
[31] Norreklit, H. (2000). The balance on the balanced scorecard a critical analysis of some of its assumptions. *Management Accounting Research.* 11(1). pp. 65-88.
[32] Grembergen, W.V. (2000). *The* Balanced Scorecard and IT Governance. *Information Systems Control Journal*. 2(1).
[33] Chapin, D.A., Akridge, S. (2005). How can security be measured? Information Systems Control Journal, Volume 2, 2005.
[34] Ozkan, S., Hackney, R., Bilgen, S. (2007). Process based information systems evaluation: towards the attributes of "PRISE". *Journal of Enterprise Information Management*. 20(6). Pp. 700-725.
[35] Information Systems Audit & Control Association. (2008). Information Security Governance: Guidance for Information Security Managers. http://www.itgi.org
[36] Mahnic, V. and Zabkar, N. (2000). The Role of Information System Audits in the Improvement of University Information Systems. *EUNIS 2000 Conference Proceedings*, Poznan, Poland, pp. 101-110. www.man.poznan.pl/ist/eunis/programme/EUNIS2000/slides/mahnic/sld007.htm
[37] Mallette, D. (2005). IT Performance Improvement with COBIT and the SEI CMM. *Information Systems Audit and Control Association (ISACA)*. http://www.isaca.org/Template.cfm?Section=COBIT_Mapping1&Template=/ContentManagement/ContentDisplay.cfm&ContentID=25094
[38] Goldman, J.E. & Ahuja, S. (2009, May). Integration of COBIT, Balanced Scorecard and SSE-CMM as a strategic Information Security Management (ISM) framework. Poster session presented at the 30th IEEE Symposium on Security & Privacy, Oakland, CA.

APPENDIX A



COBIT & BSC gaps from an ISM perspective

APPENDIX B



Mitigation of COBIT & BSC gaps + mapping of SSE-CMM