CERIAS Tech Report 2009-21

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

by Suchit Ahuja
Center for Education and Research
Information Assurance and Security
Purdue University, West Lafayette, IN 47907-2086

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

By

Suchit Ahuja

A Directed Project

Submitted in Partial Fulfillment

Of the Requirement for the Degree

of

Master of Science

Purdue University, West Lafayette

July 2009
College of Technology

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. 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 – 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 (Goldman & Christie, 2004) using ISO 27001 and SSE-CMM
- mapping of processes for effective integration of COBIT and SEI-CMM (IT Governance Institute, 2007a)
- mapping of COBIT with ITIL and ISO 27002 (IT Governance Institute, 2008) 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 information security management (ISM) that is aligned with business, IT

and information security strategies. Therefore, a valid opportunity to conduct this research study exists.

Table of Contents

List of Figures

List of Tables

List of Appendices

Acknowledgements

I am heartily thankful to my faculty advisor and chair of my advisory committee, Prof. Jim Goldman, whose guidance and support enabled me to complete this project. Prof. Goldman's vision and passion for the subject inspired me to work hard to accomplish the objectives of this project, while his unconditional support allowed me to present at reputed conferences and gather invaluable feedback on the research. I also thank Prof. Jeff Brewer and Prof. Lorenzo Martino, who have supported me as members of my advisory committee and helped me refine my work.

I offer my regards and gratitude to Prof. Khalid Moidu, for inspiring me to work towards my Master's degree and for providing me with opportunities that have contributed greatly to my knowledge, learning and growth. I also owe many thanks to my supervisor, Pam Buroff-Murr, for her unruffled support and understanding.

Lastly, I thank God; my parents, especially my mom, who has been a pillar of strength; and my friends for their love, blessings and patience.

Introduction

Threats to security of business information, information-based assets, intellectual property, and privacy of personal information are increasing. According to Privacy Rights Clearinghouse (2009), a consumer privacy protection foundation, more than 250 million records containing sensitive personal information were involved in security breaches in the U.S. since January 2005. In order to proactively deal with these growing threats and to protect the security and privacy of information-based assets, organizations are increasingly adopting information security management systems (ISMS). Although organizations use several established international standards and frameworks like ISO27001, ISO 27799, ISO27002, NIST, FIPS, ANSI, etc. for information security management, the primary driving factor for such implementations are regulatory compliance requirements (Turner, Oltsik & McKnight, 2008). In order to be compliant with requirements of applicable industry regulations like Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley (SOX), Gramm Leach Bliley Act (GLBA), Children's Online Privacy Protection Act (COPPA), Family Educational Rights and Privacy Act (FERPA), etc., organizations adopt ISMS and frameworks. The IT organization also adopts best practices and supporting tools like IT Infrastructure Library (ITIL), Control Objectives for Information Technology (COBIT), Capability maturity Model Integration (CMMI), Six Sigma, etc. for IT service, support, quality management and information security management.

The strategic integration of these frameworks and tools is not easy for the organization as successful implementation is dependent upon a range of factors, from organizational culture to training of employees (Elci, Ors & Preneel, 2008). Organizations can gain additional value and benefits by using a combination of standards and best practices (for strategic ISM). This is supported by studies showing the combination of ISO, ITIL and COBIT (Turner, Oltsik & McKnight, 2008). There are also other examples of combination of standards such as ISO and SSE-CMM that have been used for metrics based security assessment (Goldman & Christie, 2004) and other studies that show the mapping of processes for effective integration of COBIT and SEI-CMM (IT Governance Institute, 2007a). A research report released by the IT Governance Institute (2008) in collaboration with the Office for Government Commerce (OGC) maps COBIT with ITIL and ISO 27002, stating that using this combination of standards and best practices can lead to effective management and alignment of IT with business.

This study proposes the integrated use of Control Objectives for Information Technology (COBIT) and Balanced Scorecard (BSC) frameworks for strategic information security management. 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 information security management 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.

Statement of the Problem

Organizations are increasingly using ISM frameworks in order to mitigate risks and reduce threats to business assets (mainly information assets). A purely technical approach to implementation of information security controls proves insufficient in addressing the strategic objectives of the organization. As displayed in

Figure *1* below, according to the results of a Global Information Security Survey (Ernst & Young, 2008), the primary drivers for investment and implementation of such ISM frameworks are mainly regulatory compliance requirements, loss of revenue, loss of stakeholder confidence, loss to brand and reputation, etc. According to a survey by Computer Weekly (2008), the deployment of such controls is generally counter-productive as 68 percent of surveyed staff admitted to bypassing their employer's information security controls in order to do their jobs. This indicates that the investment made by the organization (for technology alone) will either provide low or inadequate returns, resulting in revenue losses and even higher operational expenditures. It also establishes the fact that there is a gap between the information security controls and the overall business and IT strategy of the organization. Hence, a more comprehensive approach to ISM is being recommended by several IT security and governance organizations.

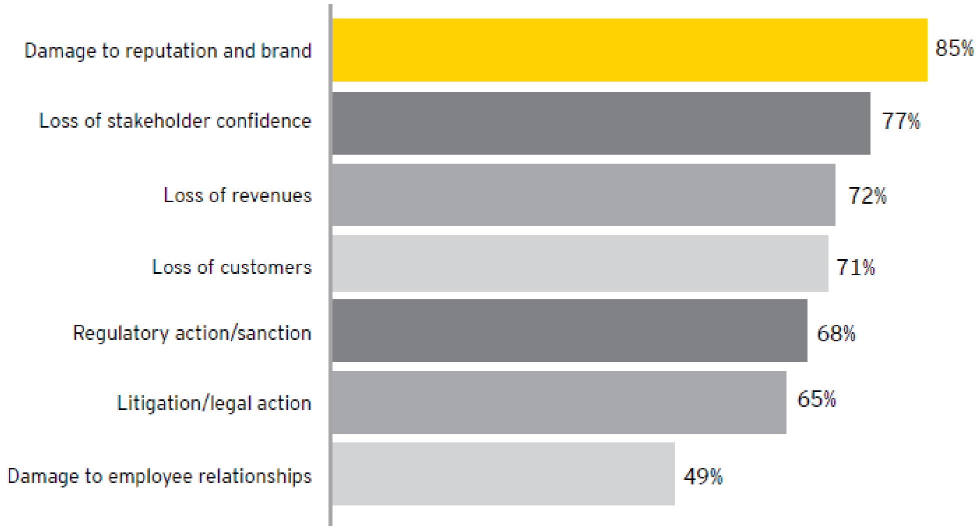

Figure 1. Primary drivers for ISM deployment (Ernst & Young, 2008).

Since the implementation of ISM frameworks is more reactive than proactive, the focus is mostly on implementation of technical controls to prevent security and privacy breaches. As a result, the strategic significance of the ISM framework is either never realized fully or the true potential to transform the business, by using the ISM framework strategically, is ignored. This leads to the existence of ISM processes and procedures that are not aligned with the business objectives of the organization. This fact is highlighted in Figure 2 below, which shows that only 18% of the organizations surveyed had information security strategy as an integrated part of their overall business strategy. The results of this survey show that alignment between business, IT and information security strategies is still not being taken into consideration while deploying ISM processes. A well-aligned approach will not only help mitigate risks and apply technical controls, but also potentially provide benefits to the business. Interestingly, a small number of organizations have started realizing the value of investing in well-aligned business, IT and information security strategies, thereby boosting investment in governance, risk and compliance management as well. According to AMR Research (2008), governance, risk management, and compliance (GRC) spending exceeded $32B for 2008, up 7.4% from 2007, as companies shift toward identifying, assessing, and managing risk across numerous business and IT areas.

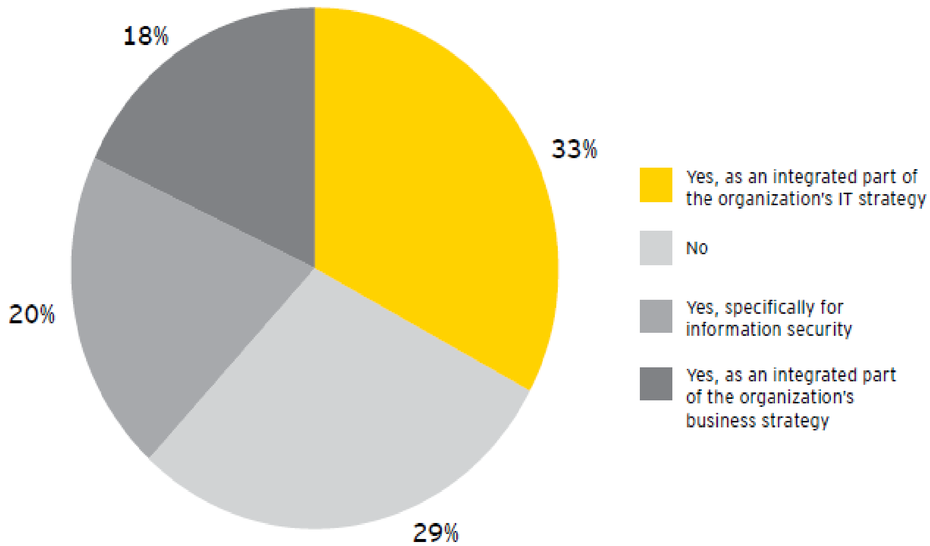

Figure 2. Perception of information security strategy (Ernst & Young, 2008).

The above discussion implies that any new ISM framework that is developed, must address not only information security processes and controls, but also the alignment of such processes and controls with an organization's overall business and IT strategies. Moreover, it is imperative to take into consideration the aspects of governance, risk and compliance to build a truly comprehensive framework. Therefore, the goal of this research study is to develop an integrated framework that addresses the need for information security requirements as well as alignment between business, IT and information security strategies.

Significance of the Problem

Strategic information security management is gaining increasing importance within organizations, becoming almost imperative as security threats continue to escalate (Sipior & Ward, 2008). According to a new study by McAfee (2009), 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. According to a survey by Deloitte Financial and Advisory Services (2009), 91% of public corporations expect fraud to increase or remain the same in 2009. The number of information security incidents reported by federal agencies jumped from 5,146 in fiscal 2006 to 12,986 in 2007, with a 70 percent increase in unauthorized access to federal networks alone, according to a report from the U.S. Office of Management (Aitoro, 2008). Figure 3 below points to an obvious lack of effective information security measures - both technical and management-focused, because regulatory compliance is often the primary driver for deployment of ISM programs within an organization (Pironti, 2006). It is critical for organizations to implement effective solutions for information security management that are based on strategic objectives. 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 policy (Siegel, Sagalow, & Serritella, 2003).

The use of tools and systems alone, can lead to gaps in an organization's business, IT and information security units. These gaps can also be further exploited due to lack of organizational IT governance mechanisms, resulting in a non-aligned approach to information security management. Although establishing an information security management system (ISMS) can address most issues, there are still certain other gaps that need to be addressed in areas like governance, alignment and management (Business Software Alliance, 2003).

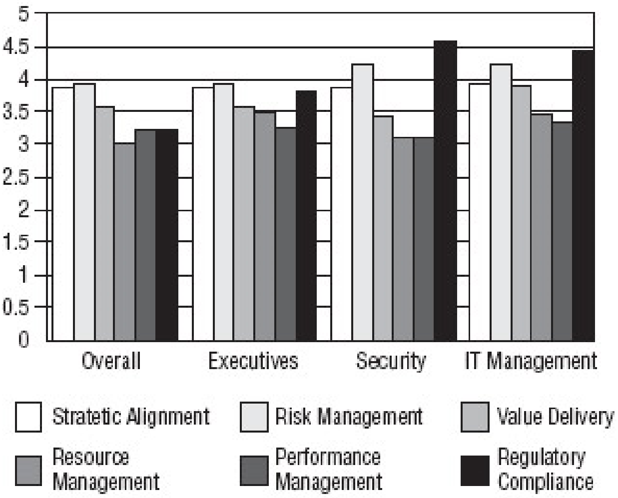

Figure 3. Significance of regulatory compliance in ISM (Pironti, 2006)

According to a survey conducted by Society for Information Management (2008), a lack of alignment of business, IT, and information security translates into lower revenues for companies. As shown in Figure 4 below, the fact stated above is further validated by an IT Governance Global Status Report (IT Governance Institute, 2008) indicating that between 2005 and 2008 the number of organizations reporting a disconnect between IT strategy and business strategy increased by almost 30%.

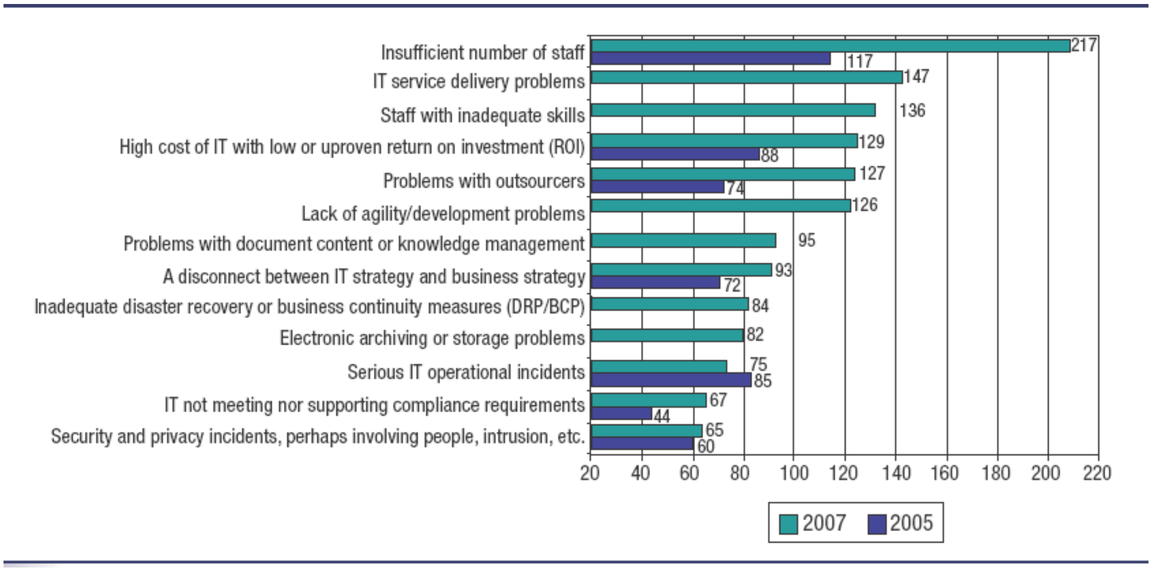

Figure 4. IT Governance global status report of 2008 (IT Governance Institute, 2008)

Another important reason for the low success rate of ISM programs across various organizations is the lack of corporate governance and ownership of information security issues. Information security management must be considered as part of the business and it is imperative to assign responsibility for managing information security to board level, as business information is a valuable and critical corporate asset. In order to mitigate risks caused by inadequate corporate governance with respect to information security management, a holistic and comprehensive framework for information security management 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 (Von Solms, 2001).

Statement of the Purpose

The purpose of this research study is to formulate an ISM framework that is aligned with business, IT and information security strategies. The main components of such an organizational ISM framework consist of:

1. Information Security Process Management and Control System

   COBIT is an international open standard that defines requirements for the control and security of sensitive data and provides a reference framework (ISACA, 2008). COBIT consists of process domains and detailed process controls that can be applied to the ISM functions within an organization. According to Von Solms (2005), COBIT positions itself as 'the tool for information technology governance' and it is therefore not exclusive to information security. It also embeds Information Security governance within a wider Information Technology governance framework, which is good because it provides an integrated platform (architecture/structure) for wider Information Technology governance. Thus, COBIT can be used to satisfy the requirement of a management and control system for ISM. According to PriceWaterhouseCoopers (2006), 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.

2. Business/IT/Information Security Alignment mechanism

   The existence of a management and control framework for ISM does not necessarily guarantee that the ISM practices are aligned with business and IT strategy. Hence, a mechanism that aligns business, IT and information security strategies is extremely crucial for the successful implementation of a comprehensive ISM framework. An ISM framework that provides robust security and controls but does not fit the organizational objectives would fail to achieve its full purpose and be detrimental to business functions. In order to avoid such a situation, it is important to use an alignment mechanism. The balanced scorecard (BSC) is a strategic planning and management system that is used extensively in business and industry, government, and nonprofit organizations worldwide to align business activities to the vision and strategy of the organization, improve internal and external communications, and monitor organization performance against strategic goals (Balanced Scorecard Institute [BSCI], 2009). The usefulness of the BSC has made it arguably the most successful and widely accepted mechanism that organizations adopt in order to achieve strategic alignment. The total usage of BSC has doubled between 1993 and 2006 with about 57% of global companies working with the BSC in one or more functions (Rigby, 2009). The use of a cascading BSC approach can lead to the effective communication of the key drivers of success to every business unit and employee within an organization, while also providing an opportunity for contribution to the overall success of an organization (Niven, 2006). Therefore, it is imperative to use a BSC approach in conjunction with COBIT, in order to align information security processes and controls with the broader business strategy and ensure the development of a strategic ISM framework.

3. Measurement and Performance Evaluation mechanism

   The implementation of a strategic framework for ISM would be incomplete if its success cannot be quantitatively measured. In order to achieve this, a standardized performance management and evaluation mechanism is required. COBIT provides a stand-alone maturity model for each of its domains, but it cannot be used as a comprehensive measurement tool (Simonsson, Johnson, & Wijkström, 2007). The SSE-CMM model describes the essential characteristics of an organization's security engineering process that must exist to ensure good security engineering (SSE-CMM.org, 2009). SSE-CMM is internationally recognized and a widely accepted model for measurement and evaluation of the maturity of security processes and controls across the organization. The deployment of an SSE-CMM approach can help the organization develop a continuous improvement approach to ISM and achieve higher levels of competence and capability as related to ISM processes and procedures.

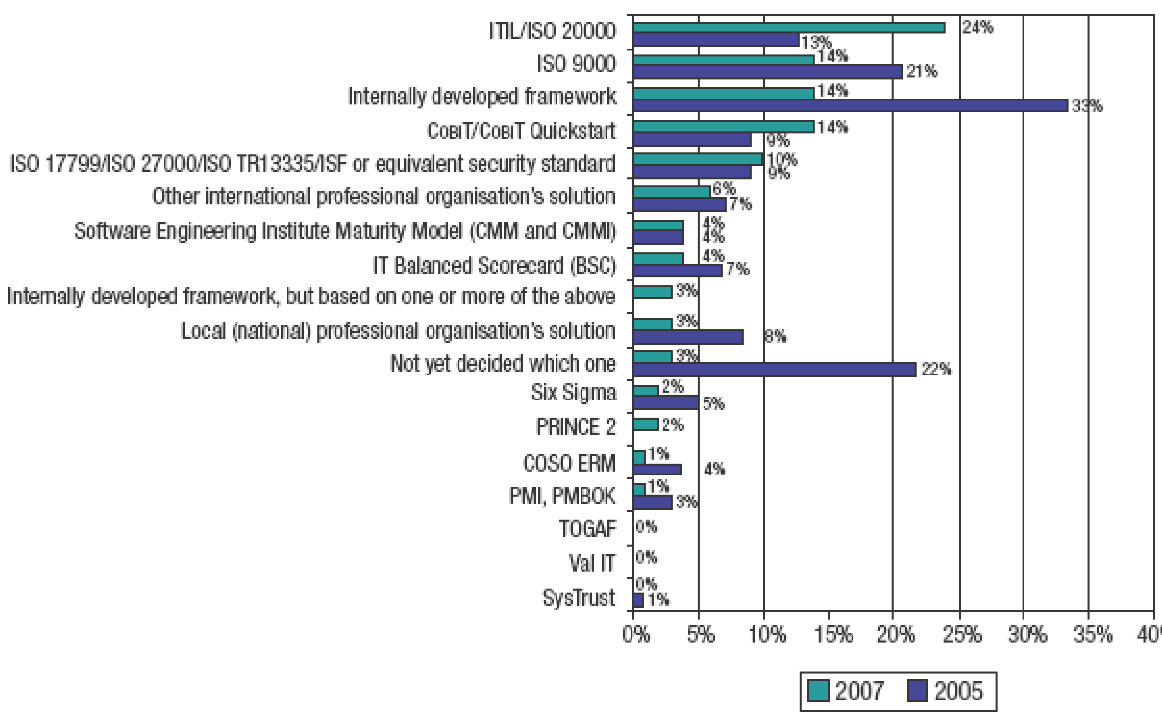

Figure 5. Solutions/Frameworks used for ISM (IT Governance Institute, 2008).

The proposed integration of COBIT, Balanced Scorecard and SSE-CMM, can potentially lead to the development of strategically aligned ISM framework. In order to fulfill the requirements for such a comprehensive framework, organizations are increasingly using an integrated approach of more than one tool or mechanism. This is evident in Figure 5 above, from the IT Governance Global Status Report (IT Governance Institute, 2008), which shows that a large number of organizations use an internally developed framework to address their ISM requirements, which usually consists of more than one internationally recognized tool or mechanism.

Definitions

Information Security Management (ISM): refers to the management of information security controls, processes, policies, people, procedures, and systems as well as the evaluation of the performance of the implemented processes.

Strategic ISM: is the integration of the ISM as a core part of the business in order to leverage it for the creation of more business opportunities in addition to managing risks and mitigating threats.

COBIT: Control Objectives for Information and related Technology (COBIT – version 4.1) is a set of best practices for information technology (IT) management that provides managers, auditors, and IT users with a set of generally accepted measures, indicators, processes and best practices for use of IT and facilitates IT governance and control in a company.

Balanced Scorecard (BSC): is a strategic alignment system that is generally used for alignment of business and IT strategies within an organization.

Cascading BSC: The cascading approach to the use of BSC can be defined as the synchronization of strategies and objectives of various business units within an organization. The business units must follow their own BSC approach, in consideration of the wider, organizational BSC approach.

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 improvements to them (sse-cmm.org, 2009)

Assumptions

The following assumptions were made for this study:

1. The study is conceptual in nature and the practical implementation can only be undertaken at a more mature stage.
2. Any organization can implement the resultant framework, but it must have some security focus.
3. The personnel responsible for implementation must be experienced in dealing with strategic alignment, IT governance or information security management.
4. The framework is flexible such that it can be customized to fit the requirements of an organization operating in any sector. However, the focus of the implementation must be mainly on the IT business unit.
5. COBIT is a huge set of best practices that cover various domains within an organization. Therefore, the organization must be familiar with COBIT requirements as it is almost impossible to implement a subset of COBIT domains while ignoring the others.
6. SSE-CMM is mainly used by organizations that do not focus on software development. If a software development organization wants to use SSE-CMM, it should first start with SEI-CMM.

Delimitations

This research study has the following delimitations:

1. The comprehensive framework will be created by integrating COBIT, Balanced Scorecard and SSE-CMM frameworks and these are a limited set of tools that were chosen from a wide range of available tools for the purpose of this study.
2. The integrated framework shall not provide metrics for each step in the framework because each organization must derive the metrics from its deployed strategy.
3. The metrics, targets, initiatives, KPIs, CSFs, etc. are also organizationally dependent but can be taken from the researched literature.

Limitations

This research study has the following limitations:

1. The study will be limited to proposing an integrated framework and thus the framework may not be practically validated.
2. Risk management approaches shall not be elaborated on in the proposed framework because risk management is covered in at least one of the COBIT domains and can be covered by BSC as well. It is up to the organization to choose its specific risk management approach.

Review of Literature

Purpose of COBIT: IT Governance or Security Controls?

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 (Ridley, 2004; Larsen, et. al., 2006; Debraceny, 2006). However, this perspective does not provide details about how COBIT can support a business-IT-security alignment strategy or how IT security controls can be implemented.

The definition for IT Governance provided by Massachusetts Institute of Technology (MIT), through its Sloan School of Management's Center for Information Systems Research (CISR) points out that IT Governance specifies the decision making rights and the framework of responsibilities to promote desirable behavior in the use of IT (Weill & Ross, 2004). 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. According to Curtis and Wu (2000), COBIT was developed to "bridge the gap" between currently existing business-control models and IT-control models. This purpose has been overshadowed by the more popular opinion that COBIT is purely a management tool used to ensure effective IT finance and governance by senior management (IT Governance Institute, 2007).

According to published material in the Proceedings of the 12th European Conference on Information Technology Evaluation (Remenyi, 2005), implementing COBIT areas and processes was difficult due to the lack of defined "ownership" of the processes. This is a problem in mapping corporate governance to IT governance and even if COBIT does not prescribe "process ownership", such a problem highlights the lack of alignment between organizational and governance objectives. In contrast, according to Schlarman (2007), COBIT lacks the tactical direction that some organizations need in strategic ISM areas. Haes and Grembergen (2005) provided an illustration 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. Hence, the solution remained incomplete in terms of business-IT-security alignment.

Strengths of COBIT

According to Rouyet-Ruiz (2008), 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. As an advantage, these fields are inherently defined in process orientation and in the structured metrics system that measures those processes. COBIT has become a de-facto standard especially in financial organizations (Robinson, 2005) thereby making it universally applicable. It is a comprehensive, independent, evolving, large body of knowledge and educational support. It has a common language and maturity model (when used in combination with CMM) for IT process improvement (Lainhart 2000; ITGI 2007). There are many examples of using COBIT in conjunction with SEI-CMM in order to measure the maturity of processes within an organization (ITGI, 2007; Mallette, 2005). 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 (Haes & Grembergen, 2005).

Weaknesses of COBIT

Although IT governance is considered to be an enabler for business/IT alignment, according to Rouyet-Ruiz (2008) and Ernest (2007), COBIT lacks in the establishment of responsibilities and a methodological alignment with the business strategy – especially when COBIT processes are used for enabling information security strategy management. This is by far the biggest gap that needs to be plugged by using another framework; otherwise the purpose of using COBIT would be defeated if the recommended controls and processes are not aligned with business strategy. Simonsson, Johnson & Wijkström (2007) further state the following weaknesses:

- COBIT contains all the processes, activities, documents, etc. needed to represent all IT Governance concerns. Nonetheless, some incongruence exists within COBIT like control objectives not being effectively mapped to process areas and not aligned with business requirements.
- COBIT provides a vast amount of metrics that can be used to assess the maturity of IT governance. 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. Analysis and data collection are not clearly separated and must both be carried out by experienced analysts.

- 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.
- COBIT uses a maturity model that is mainly a stand-alone analysis tool that provides only a very shallow analysis. Due to this constraint, it takes an experienced analyst to conduct a credible maturity assessment of an IT organization by the use of COBIT.

According to Ritchie (2004), COBIT is not fully prescriptive in its methodology in order to match the control objectives with specific technology-level controls. It is a very broad framework for implementation of organizational processes. The CPA Journal (Curtis & Wu, 2000) states that 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. The downside of using COBIT for Information Security governance is that it is not always very detailed in terms of 'how' controls can be implemented (Von Solms, 2005; Lainhart, 2000).

Purpose of Balanced Scorecard (BSC)

Balanced Scorecard (Kaplan & Norton, 1996) 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 follow-up (Grembergen & Haes, 2005) as shown in Figure 6 below. The balanced scorecard usually consists of four specific domains as listed below and displayed in Figure 7 below.

1. the business contribution perspective capturing the business value created from various investments (in the context of this research study, security investments will also be considered)
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

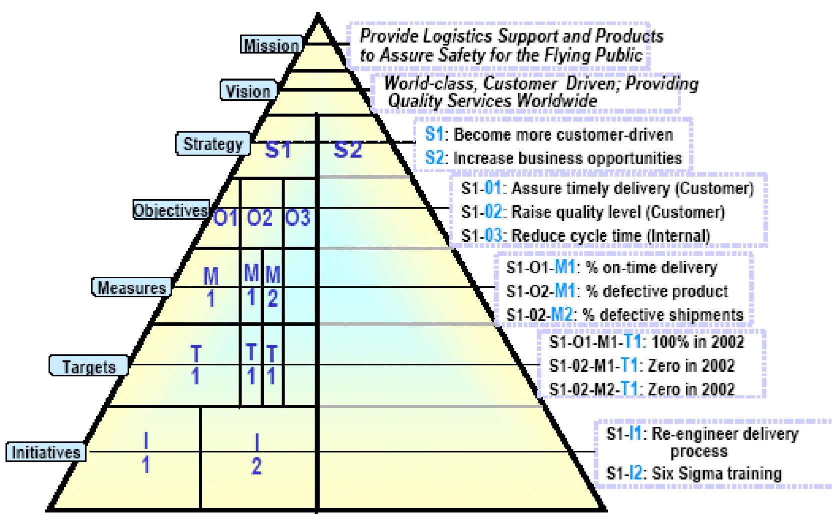

Figure 6. Balanced Scorecard pyramid. (Kaplan & Norton, 1996).

The domains can be tweaked to fit the information security strategy. In order to achieve business-IT-information security alignment (Microsoft, 2007), it is important to use the cascading BSC approach. 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 result should be to focus across all levels of the organization that is consistent. An example of a cascading BSC is shown in Figure 8 below. The organization alignment should be clearly visible through strategy, using the strategy map, performance measures and targets, and initiatives. Scorecards are used to improve accountability through objective and performance measure ownership, and desired employee behaviors are incentivized with recognition and rewards."

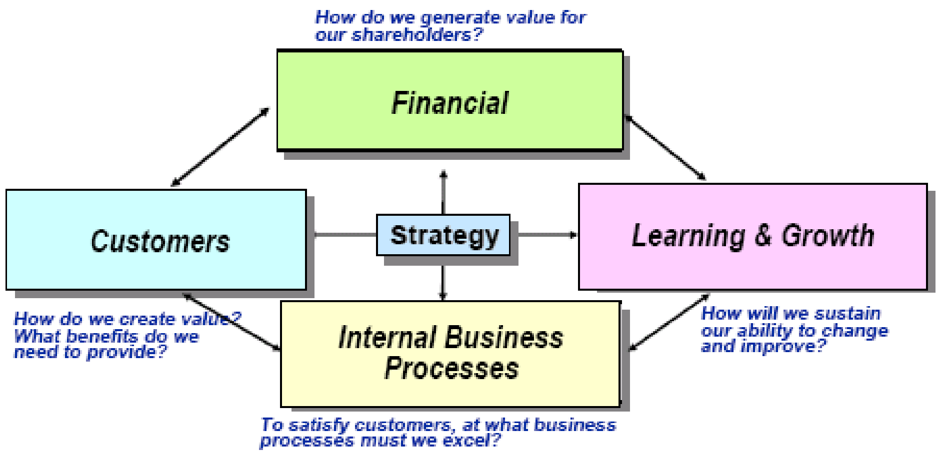

Figure 7. Balanced Scorecard domains. (Kaplan & Norton, 1996)

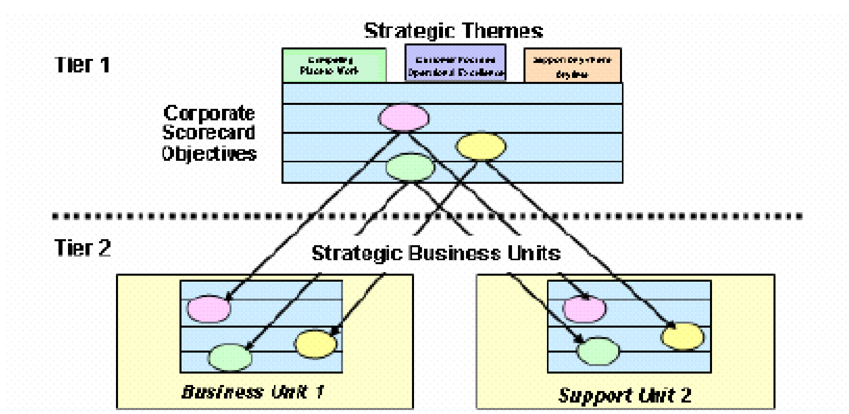

Figure 8. Balanced Scorecard cascade. (Kaplan & Norton, 1996)

As demonstrated by Cobbold and Lawrie (2002), BSC has gone through an evolution and there has been extensive research to fine-tune the original BSC approach and implement it. This process can help achieve a better fit for the organization and provide a customized scorecard that can produce improved results. The cascading balanced scorecard approach (between business and IT) can be successfully used as a strategic management tool (Kaplan, 1996; Kaplan, 2005; Martinsons, 1999).

Weaknesses of BSC

The BSC approach to effective strategic management is often seen as subjective and difficult to implement. According to Malina and Selto (2001), 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. It can be hard to provide evidence of causal relations between effective management control, motivation, strategic alignment and beneficial effects of the BSC. Ineffective communication and management control cause poor motivation and conflict over the use of the BSC as an evaluation device (Ahn, 2001; Malina & Selto, 2001). There is disagreement about how the balanced scorecard can link strategy to operational metrics, which managers can understand and influence (Norreklit, 2000). Considering an ISM perspective and the context of this research study, 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 indicates that BSC is a multi-purpose tool that can be used as a performance management system (Rohm & Halbach, 2005), IT governance mechanism (Grembergen, 2000) and as a strategic alignment framework (Kaplan & Norton, 1996). BSC is a powerful framework for aligning business/IT strategy, but when it is used as a standalone mechanism for comprehensive alignment of business/IT/security strategies, its weaknesses and gaps are exposed. These weaknesses range from management conflicts due to lack of an ideal set of parameters for information security (that the BSC must operate on) to the lack of a reporting mechanism for low-level information security metrics. Similarly, COBIT is highly effective when used as a standalone mechanism for IT governance, but is lacking when assessed from a business/IT alignment perspective. To that end, if COBIT is used for business/IT/information security alignment purposes, the gaps in business/IT alignment must be plugged before the security control objectives that are prescribed by COBIT process areas can be implemented.

The importance of security measurement and performance evaluation

It is difficult to measure security controls and security processes, both qualitatively and quantitatively (Wang & Wulf, 1997; Chapin & Akridge, 2005; Ozkan, Hackney & Bilgen, 2007). It is extremely crucial to measure the performance of processes that are deployed for information security management, in conjunction with security controls, in order to derive accurate results. According to Chapin and Akridge (2005), traditionally risk assessment, risk mitigation, and residual risk were used as mechanisms to balance security risks and requirements, considering business needs, budget, and other resources. Further, with the advent of globalization, business structures have become more complex, with outsourcing and off-shoring now acting as business drivers, and increased levels of global threats to information security. In order to counter such 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 (AMR Research, 2008). 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 & Christie, 2004).

The success of such a security measurement and performance evaluation approach is significantly dependent upon tracking and reporting of accurate security metrics. The key to the strategic use of security metrics is to obtain measurements that have the following ideal characteristics (Chapin & Akridge, 2005):

- They should measure organizationally meaningful things
- They should be reproducible
- They should be objective and unbiased
- Over time, they should be able to measure some type of progression toward a goal

The accurate use of information security "process and control metrics" can lead to better return on investment (for security investments), while moving the organization towards a continuous improvement approach – thereby ensuring the sustainability of the security management practices. To that end, there is requirement of an ISM process maturity framework, which is applicable across the organization and is deployed from a strategic perspective. This requirement can be fulfilled by the SSE-CMM maturity model as it facilitates synergy between system life cycle phases, increases efficiency, reduces wastage, and results in more secure solutions with greater assurance and lower costs (Goldman & Christie, 2004).

Various frameworks for measuring security maturity are widely used in areas like software engineering and information technology as shown in Figure 9 below (Ozkan, Hackney & Bilgen, 2007). Nonetheless, each framework has its own advantages and disadvantages, while adoption is dependent on a set of organizational requirements. 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 (Simonsson, Johnson & Wijkström, 2007). In contrast, 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.

Model	Description	Comments
NIST CSEAT IT Security Maturity Model[2]	Five levels of progressive maturity: 1. Policy 2. Procedure 3. Implementation 4. Testing 5. Integration	Focused toward levels of documentation
Citigroup's Information Security Evaluation Model (CITI-ISEM)[3]	Five levels of progressive maturity: 1. Complacency 2. Acknowledgment 3. Integration 4. Common practice 5. Continuous improvement	Focused toward organizational awareness and adoption
CobiT® Maturity Model[4]	Five levels of progressive maturity: 1. Initial/*ad hoc* 2. Repeatable but intuitive 3. Defined process 4. Managed and measurable 5. Optimized	Focused toward auditing specific procedures
SSE-CMM Model[5]	Five levels of progressive maturity: 1. Performed informally 2. Planned and tracked 3. Well-defined 4. Quantitatively controlled 5. Continuously improving	Focused toward security engineering and software design
CERT/CSO Security Capability Assessment[6]	Five levels of progressive maturity: 1. Exists 2. Repeatable 3. Designated person 4. Documented 5. Reviewed and updated Measures using four levels: 1. Initial 2. Evolving 3. Established 4. Managed	Focused toward measurement of quality relative to levels of documentation

Figure 9. List of Maturity Models for Security (Ozkan, Hackney & Bilgen, 2007).

The objective of the SSE-CMM is to advance security engineering as a defined, mature, and measurable discipline by leveraging the following key factors (SSE-CMM.org, 2009):

- The organization must be able to justify focused investments in security engineering tools, training, process definition, management practices, and improvements.

- Capability-based assurance or trustworthiness based on confidence in the maturity of an organization’s security practices and processes
- Selection of appropriately qualified providers of security processes through differentiating by capability levels and associated programmatic risks

Figure 10 below, shows a comparison between SSE-CMM and various other security maturity models in terms of their goals, approaches, and benefits. SSE-CMM applies a comprehensive engineering-based approach to security measurement (SSE-CMM.org, 2009). This provides good justification, in part, for its use in a diverse process area /domain specific environment such as the one being studied in this research project.

Effort	Goal	Approach	Scope	Status
SSE-CMM	Define, improve, and assess security engineering capability	Continuous security engineering maturity model and appraisal method	Security eng. organizations	Version 3.0
SE-CMM	Improve system or product engineering process	Continuous maturity model of systems eng. practices and appraisal method	Systems eng. organizations	See EIA731
SEI CMM for Software	Improve the management of software development	Staged maturity model of software engineering and management practices	Software eng. organizations	Now in CMMI
Trusted CMM	Improve the process of high integrity software development and its environment	Staged maturity model of software engineering and management practices including security	High integrity software organizations	Unknown
CMMI	Combine existing process improvement models into a single architectural framework.	Sort, combine, and arrange process improvement building blocks to form tailored models	Engineering organizations	Partial draft released
Sys. Eng. CM (EIA731)	Define, improve, and assess systems engineering capability	Continuous systems engineering maturity model and appraisal method	Sys. eng. organizations	Released
Common Criteria	Improve security by enabling reusable protection profiles for classes of technology	Set of functional and assurance requirements for security, along with an evaluation process	Information technology	Version 2.0
CISSP	Make security professional a recognized discipline	Security body of knowledge and certification tests for security profession	Security practitioners	In use
Assurance Frameworks	Improve security assurance by enabling a broad range of evidence	Structured approach for creating assurance arguments and efficiently producing evidence	Security engineering organizations	Research papers
ISO 9001	Improve organizational quality management	Specific requirements for quality management practices	Service organizations	In wide use
ISO 15504	Software process improvement and assessment	Software process improvement model and appraisal methodology	Software eng. organizations	All 9 parts published
ISO 13335	Improvement of management of information technology security	Guidance on process used to achieve and maintain appropriate levels security for information and services	Security engineering organizations	3 of 5 parts published

Figure 10. Comparison of SSE-CMM to related models (SSE-CMM.org, 2009).

Conclusion of Review of Literature

The research in the literature review highlights previous studies that show the strengths of the cascading balanced scorecard approach, for alignment between business-IT-information security strategies. On the other hand, the weaknesses (when used as a standalone approach) highlighted range from lack of information governance to conflicts in prioritization of implementation of objectives. Similarly, the strengths of COBIT that are highlighted include enabling IT governance (including information assets), comprehensive approach to process controls, and an audit-based approach to information security. The weaknesses of COBIT (when used as a standalone approach) are that the processes within each of COBIT’s process domains are not aligned with the overall business strategy and this may lead to ineffectiveness in the application of information security controls (Rouyet-Ruiz, 2008; Ernest, 2007). This may prove to be a detrimental factor while conducting information security audits, as the results potentially may not be useful to the business.

The challenge is to formulate an integrated framework for ISM, using both cascading BSC and COBIT, to enable a comprehensive approach that is aligned with the strategic business focus of the organization. The ISM framework itself would not be able to provide meaningful audit-based performance evaluation reports to the business, solely based on the COBIT control objectives that are applied to information security processes. Therefore, 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.

Procedures

This study is based on the conceptual development of a comprehensive framework for ISM using cascading BSC, COBIT, and SSE-CMM. 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. Gap analysis of COBIT and BSC frameworks
2. Mitigation of gaps based on previous research and added value from current efforts
3. The formulation of the integrated framework

Gap Analysis of COBIT and BSC frameworks

A gap analysis of COBIT and BSC frameworks (standalone), from the perspective of their potential use in an ISM framework (Goldman & Ahuja, 2009) was conducted. The standalone use of the cascading BSC approach (as shown in *Figure 11* below) and the standalone use of COBIT (as shown in *Figure 12* below) highlight the general gaps of both frameworks from an ISM perspective, taking into account the audit-based approach required to achieve an effective and integrated solution. A consolidated list of gaps that exist in both frameworks was derived (as shown in Table 1 below) and potential mitigation mechanisms were suggested based on previous studies and research, as discussed in the review of literature.

Mitigation of Gaps based on previous research and added value from current efforts

The mitigation of gaps that are derived from *Figure 11* and *Figure 12* (also listed in Table 1) can be conducted by either addressing each one separately or by grouping them together (wherever synergies exist in the processes):

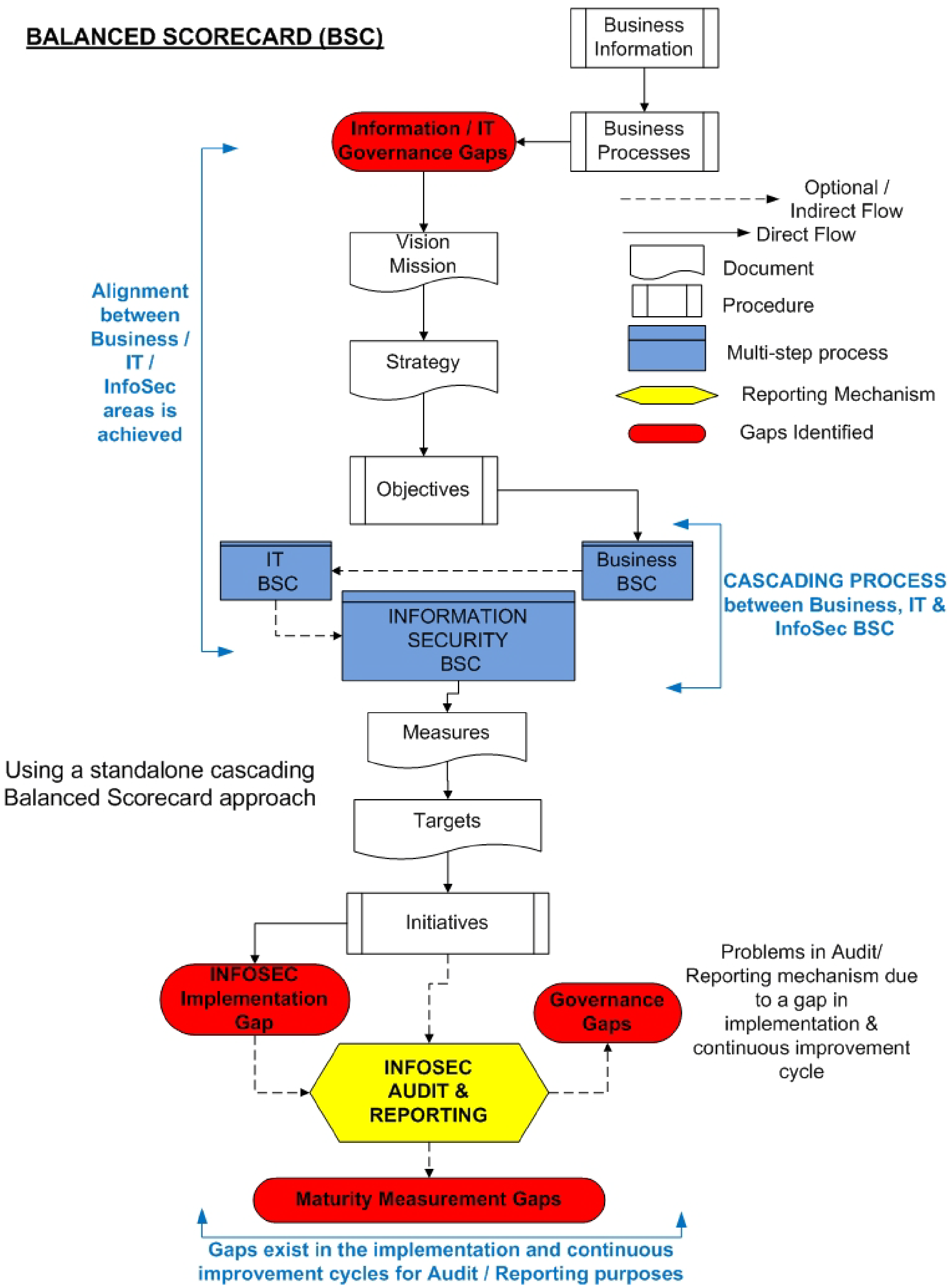

Figure 11. Cascading BSC Gaps (Goldman & Ahuja, 2009)

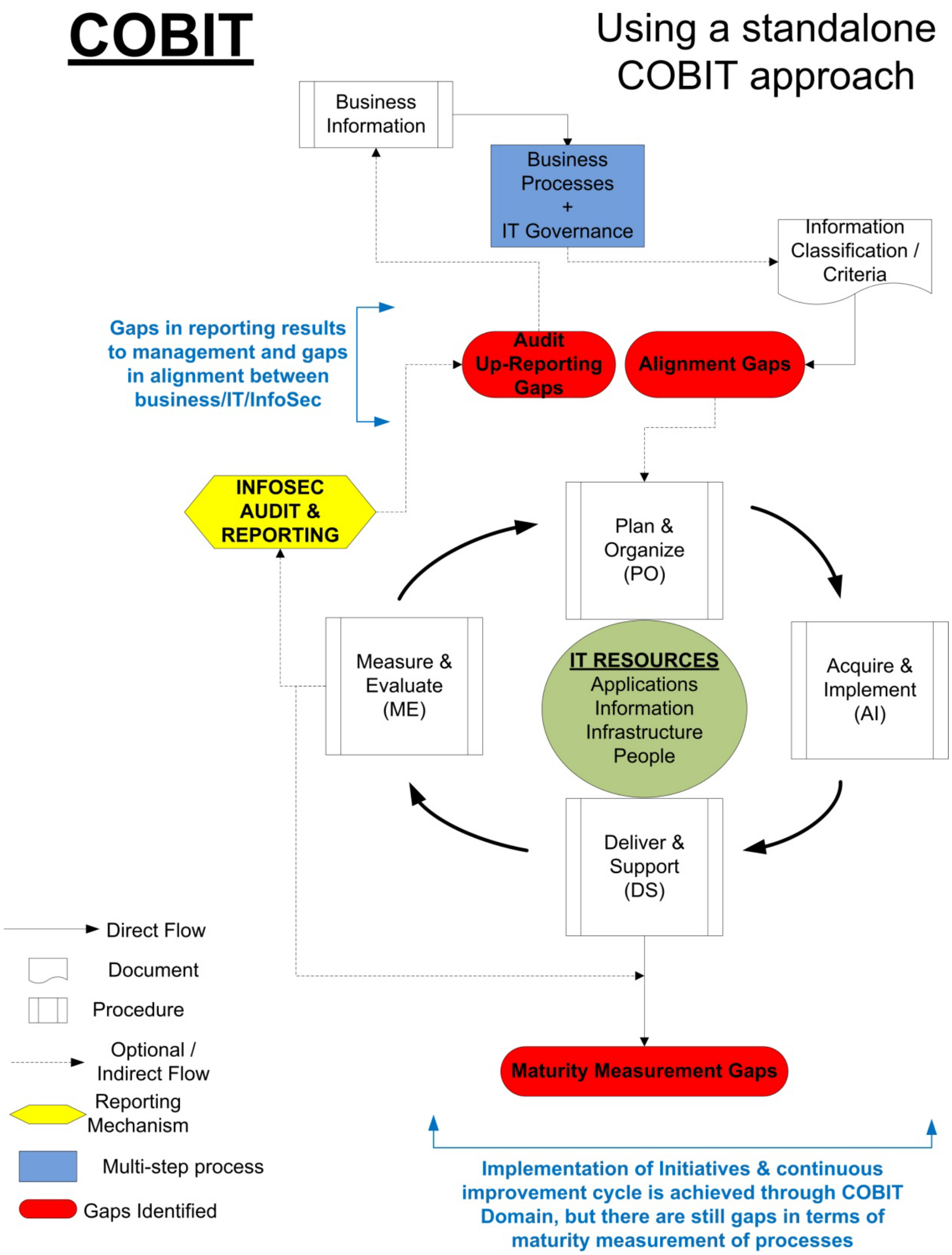

Figure 12. COBIT Gaps (Goldman & Ahuja, 2009)

i. Gap #1.1: A gap in the alignment of business, IT and information security strategies can be addressed by creating a mapping between those COBIT process areas that address the formulation of a strategic IT plan and a cascading BSC approach. The aim is to demonstrate that a cascading BSC approach can enable the implementation of the alignment. Appendix A – Cascading balanced scorecard example provides an illustration of the cascading BSC approach aligning business, IT and information security strategies for a healthcare organization. It is important to distinguish between the application of the COBIT and BSC frameworks, at the tactical and strategic organizational levels respectively, as shown by Da Cruz and Labuschagne (2006) as shown in *Figure 13* below. BSC is generally used to determine the strategy of the organization in terms of its business, IT and ISM goals, while COBIT is used to implement the strategy tactically, using its “best practices” methodology. These two frameworks (and their usage at respective levels in the organization) are not interchangeable.

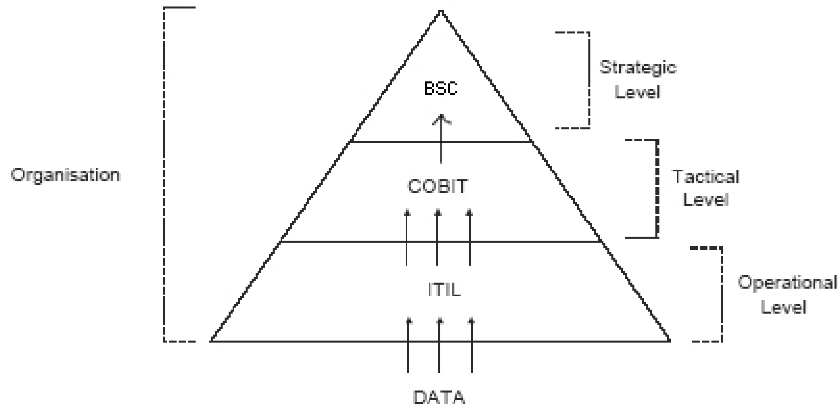

Figure 13. Application of frameworks at different levels of the organization for security management (Da Cruz & Labuschagne, 2006)

ii. Gap #1.2, 2.2: Using the methodology provided by Grembergen and Haes (2005) to map the organizational Key Performance Indicators (KPIs) and Key Goal Indicators (KGIs) to the BSC initiatives and COBIT domain "Monitor & Evaluate", this gap can be mitigated. An example is shown in Figure 14 below. The approach can establish traceability between the metrics defined at the business level via the BSC approach and tie them directly to organizational KPIs, KGIs as well as the metrics used in the COBIT processes. An important consideration at this stage is that COBIT is only a "best practices" or "control" framework for security processes within the scope of this study. The concrete security metrics will come from the underlying physical security controls that must then be translated into meaningful organizational metrics in order to be useful to the business. This process can be facilitated via mitigation of gap #1.2 as well. In order to address gap #2.2, specific attention must be paid to COBIT domain "Measure & Evaluate" in order to implement the process correctly for collection of the required security metrics that must be reported to management.

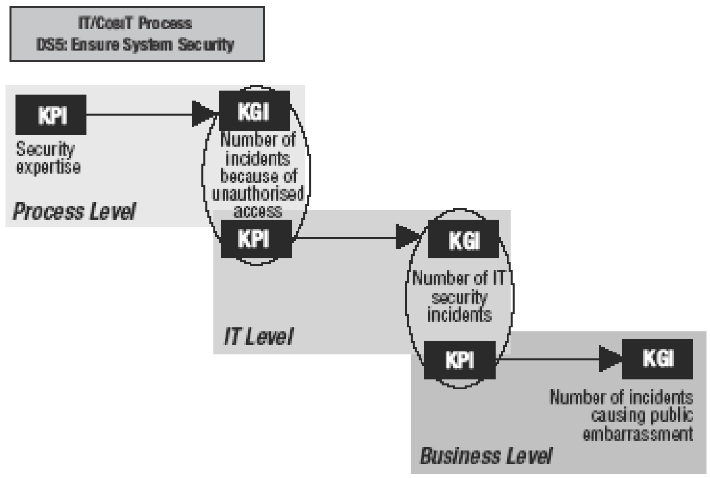

Figure 14. Information Security KPI & KGI mapping to business level (Grembergen & Haes, 2005)

iii. Gap # 1.3, 1.4, 2.3, 2.4: The combined use of methodology specified by Goldman and Christie (2004), Mallette (2005), IT Governance Institute (2007a), and IT Governance Institute (2008) can help mitigate these gaps. The basic idea is to create a mapping between COBIT domains and SSE-CMM process areas such that the organization can use this to streamline the common functions and better understand the processes that need to tracked and aligned in order to achieve an efficient ISM approach. Goldman & Christie (2004) used SSE-CMM and ISO 17799 for metrics based evaluation, therefore the ten SSE-CMM PAs (Process Areas) can be re-used in this study (as shown in Figure 15 below), instead of considering the whole set. The other studies primarily used SEI-CMM (which is primarily used to measure software development process maturity) to map to COBIT domains. A potential solution would be to use the methodology and replace SEI-CMM PAs with SSE-CMM PAs. A sample table with a mapping structure is shown in Figure 18: SSE-CMM (v. 3.0) Capability Maturity Levels

iv. below. It must be noted that this table is a summary table and the creation of a detailed table would be required in order to ensure that each COBIT domain and each process within each domain is mapped correctly. Similar consideration would apply for the SSE-CMM PAs as well.

SSE-CMM Process Area	Description
PA 01	Administer Security Controls
PA 02	Assess Operational Security Risk
PA 03	Attack Security
PA 04	Build Assurance Argument
PA 05	Coordinate Security
PA 06	Determine Security Vulnerabilities
PA 07	Monitor Security Posture
PA 08	Provide Security Input
PA 09	Specify Security Needs
PA 10	Verify and Validate Security

Figure 15. SSE-CMM Process Areas (Goldman & Christie, 2004)

However, after 2004, in the newer version (v. 3.0) of SSE-CMM the process areas have been slightly modified. These are displayed in Figure 16 below.

SSE-CMM (v. 3.0) Process Area	Description
PA 01	Administer Security Controls
PA 02	Assess Impact
PA 03	Assess Security Risk
PA 04	Assess Threat
PA 05	Assess Vulnerability
PA 06	Build Assurance Argument
PA 07	Coordinate Security
PA 08	Monitor Security Posture
PA 09	Provide Security Input
PA 10	Specify Security Needs
PA 11	Verify and Validate Security

Figure 16. SSE-CMM (v. 3.0) Process Areas

In addition to the above, SSE-CMM (v3) also includes eleven process areas related to project and organizational practices. These process areas and the base practices that define them are listed in Figure 17 below.

SSE-CMM (v. 3.0) Process Area	Description
PA 12	Ensure Quality
PA 13	Manage Configuration
PA 14	Manage Project Risk
PA 15	Monitor and Control Technical Effort
PA 16	Plan Technical Effort
PA 17	Define Organization's Systems Engineering Process
PA 18	Improve Organization's Systems Engineering Process
PA 19	Manage Product Line Evolution
PA 20	Manage Systems Engineering Support Environment
PA 21	Provide Ongoing Skills and Knowledge
PA 22	Coordinate with Suppliers

Figure 17: SSE-CMM (v. 3.0) Process Areas (focusing on organization and project management)

Maturity levels represent the attributes of mature security engineering necessary to achieve each level. These maturity levels are listed in Figure 18Figure *18*: SSE-CMM (v. 3.0) Capability Maturity Levels

below:

SSE-CMM Maturity Level	LEVEL	Description
Level 1	1.1	Base Practices are Performed
Level 2	2.1	Planning Performance
	2.2	Disciplined Performance
	2.3	Verifying Performance
	2.4	Tracking Performance
Level 3	3.1	Defining a Standard Process
	3.2	Perform the Defined Process
	3.3	Coordinate the Process
Level 4	4.1	Establishing Measurable Quality Goals
	4.2	Objectively Managing Performance
Level 5	5.1	Improving Organizational Capability
	5.2	Improving Process Effectiveness

Figure 18: SSE-CMM (v. 3.0) Capability Maturity Levels

CobiT Processes	SEI CMM KPAs High-level Correlation	SEI CMM KPAs Correlated to CobiT Through Activity and Intent	CobiT Detailed Control Objectives Fulfilled	Percent of CobiT Fulfilled With SEI CMM	Percent of KPAs to CobiT
Plan and Organize					
PO1 Define a strategic plan	IC	TCM	5 of 8	63%	11%
PO2 Define the information architecture			0 of 4	0%	0%
PO3 Determine technological direction	TCM	TCM	4 of 5	80%	6%
PO4 Define the IT organization and relationships	IC	OPF,OPD, IC, TCM,SSM	6 of 15	40%	28%
PO5 Manage the IT investment		TCM	1 of 3	33%	6%
PO6 Communicate management aims and direction		PCM	6 of 11	55%	6%
PO7 Manage human resources			0 of 8	0%	0%
PO8 Ensure compliance with external requirements		RM	1 of 6	17%	6%
PO9 Assess risks	SPP, ISM	SPP, PTO, ISM	6 of 8	75%	17%
PO10 Manage projects	SPP, PTO, ISM	SPP, PTO, ISM, SQA, SPE	14 of 14	100%	28%
PO11 Manage quality	SQA, OPF, SQM, TP, ISM	SQA, OPF, SQM, TP, ISM, QPM	16 of 19	84%	33%
Acquire and Implement					
AI1 Identify automated solutions	RM, TCM	RM, SPE, TCM	4 of 18	22%	17%
AI2 Acquire and maintain application software	SPE, SSM, SCM	SPE, SSM, SCM, RM	6 of 17	35%	22%
AI3 Acquire and maintain technology infrastructure	SCM, TCM, PCM	SCM, TCM, SSM	3 of 6	50%	17%
AI4 Develop and maintain procedures	ISM, OPF, OPD	OPF, OPD, PCM, SPE, ISM	3 of 4	75%	28%
AI5 Install and accredit systems	SPE	SPE, ISM	6 of 14	43%	11%
AI6 Manage changes	SCM, PCM, TCM	SCM	5 of 8	63%	6%
Deliver and Support					
DS1 Define and manage service levels			0 of 7	0%	0%
DS2 Manage third-party services	SSM	SSM	6 of 8	75%	6%
DS3 Manage performance and capacity			0 of 9	0%	0%
DS4 Ensure continuous service		SPP,ISM	3 of 13	23%	11%
DS5 Ensure systems security			0 of 21	0%	0%
DS6 Identify and allocate costs	SPP, PTO	SPP, PTO, ISM	3 of 3	67%	17%
DS7 Educate and train users	OPD, TP	OPD, TP,SPE	2 of 3	67%	17%
DS8 Assist and advise customers		SQA	2 of 3	67%	6%
DS9 Manage the configuration	SCM	SCM	6 of 8	75%	6%
DS10 Manage problems and incidents	DP	DP	3 of 5	60%	6%
DS11 Manage data	SPP, PTO, ISM	SPP, PTO, ISM	3 of 30	10%	17%
DS12 Manage facilities			0 of 6	0%	0%
DS13 Manage operations	IC		0 of 8	0%	0%
Monitor and Evaluate					
M1 Monitor the processes	QPM, PCM	QPM, PCM	4 of 4	100%	11%
M2 Assess internal control adequacy	SQA	SQA	3 of 4	75%	6%
M3 Obtain independent assurance	SQA, PR	SQA, PR,SSM	6 of 8	75%	17%
M4 Provide for independent audit		SQA	4 of 8	50%	6%

Legend: SEI CMM KPAs Used in Correlation Matrix

DP: Defect prevention
IC: Intergroup coordination
ISM: Integrated software management
OPD: Organization process definition
OPF: Organization process focus
PCM: Process change management
PTO: Project tracking and oversight
QPM: Quantitative process management
RM: Requirements management
SCM: Software configuration management
SPE: Software product engineering
SPP: Software project planning
SQA: Software quality assurance
SQM: Software quality management
SSM: Software subcontract management
TCM: Technology change management
TP: Training program

Figure 19. COBIT domains mapping with SEI-CMM PAs - summary chart (Mallette, 2005)

v. 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)
- Reliability (R)

A comparison of this with other mechanisms for information governance, like the Information Criticality Matrix (ICM), which is part of the Infosec Assessment Methodology (IAM) developed by the National Security Agency (NSA), can provide some insight into the use of COBIT for information governance. It enables the prioritization of information (and information asset) protection based on criteria set by the organization from a business perspective, and thus helps resolves any conflicts that may arise due to personal misinterpretation by executive management.

The formulation of the integrated framework

The true integration of COBIT, cascading BSC, and SSE-CMM can be shown with a comprehensive illustration of the mitigation of the gaps from the standalone frameworks. The gaps must not only be mitigated individually, but they must also help to enable the integration of the three frameworks. In order to justify that the individual components of the comprehensive framework are functionally correct, more illustrations with respect to established research studies can be provided. Finally, a high-level diagram showing the integrated summary of the research (i.e COBIT, cascading BSC, and SSE-CMM) contributing to the successful implementation of a strategic ISM framework would ensure that the solution is universally understandable and not just restricted to technical staff or security experts.

COBIT – BSC Gap Analysis

In order to design an integrated framework that uses COBIT and BSC, the gaps that exist within each tool individually must be studied. In order to highlight these gaps, both frameworks must be analyzed separately. Figure 11 and Figure 12 above show the various components of COBIT & BSC frameworks when used individually, following a top-down approach starting from business information and going down to 'information security management' processes and controls.

The two scenarios established in Figure 11 and Figure 12 above, highlight the gaps of both frameworks. These gaps can be potentially mitigated, by using the two frameworks in conjunction.

Scenario 1: The standalone use of Balanced Scorecard (BSC) in order to achieve alignment between business strategy, IT strategy, and ISM strategy.

The mission and vision of the business are the driving factors behind the BSC approach. The purpose of existence of the organization is determined by its mission and the value of the services it aims to provide is detailed in the vision. A strategy document that is drafted and formulated by upper management ensures that the mission and vision are durably supported throughout the organization. This is a general strategy for the whole organization and may be fine-tuned by various business units and departments within the organization to fit their purpose. Department-level (e.g. IT) objectives can be framed and every business unit can follow its own specific objectives in accordance with those listed in the broader organization-wide document. A cascading BSC approach may be used for aligning the business strategy to the IT strategy and for further alignment of IT strategy with information security strategy. The objectives of business BSC and IT BSC can be adopted in the information security BSC with appropriate relevance.

Information security BSC is closest to the operational level of the organization and metrics defined at the business-level can be applied via the information security BSC. Targets are benchmarks set by management (for each objective) and can be tweaked according to the business unit and organizational requirements.

At this point, the following gaps and weaknesses in the BSC approach are observed:

1. The initiatives can be either a set of controls (applications, systems, etc.) or a set of processes. However, BSC does not fulfill all requirements for implementation of the set of initiatives as the critical aspect of "how" the initiatives must be implemented is missing.
2. The conversion of the overall initiatives into information security initiatives that are well aligned with the business are performed by using the BSC approach. Nevertheless, additional tools or frameworks are required in order to ensure that a process lifecycle is established for the management of initiatives (either individually or as a set).
3. BSC traceability terminates at the "Initiatives" level without indicating the processes that need to be implemented.
4. Ad-Hoc BSC implementation can cause disagreement and tension between top and middle management regarding the appropriateness of specific aspects of BSC, as a communication, control and evaluation mechanism.
5. Audit and Information Security reporting gaps that can lead to lack of information flow between upper management and implementation teams.

Table 1 below lists the above gaps and weaknesses while providing potential mitigation solutions.

Scenario 2: The standalone use of COBIT for information security management

COBIT has always been projected as an IT governance framework, although it prescribes more than 200 process controls. According to the IT Governance Institute (ITGI, 2007), COBIT enables clear policy development and good practice for IT control throughout organizations. COBIT emphasizes regulatory compliance, helps organizations to increase the value attained from IT and enables alignment. COBIT is a comprehensive model for enterprise control of the IT environment / IT Governance and is divided into four domains:

1. Planning and Organization (PO)
2. Acquisition and Implementation (AI)
3. Delivery and Support (DS)
4. Monitor and Evaluate (ME)

Each of the above four domains consists of several detailed processes that recommend control objectives in order to create a mapping among the various areas within an organization. The information being processed in the four domains can be classified into the following criteria in order to provide a map for rating information criticality:

1) Effectiveness (EFT)
2) Efficiency (EF)
3) Confidentiality (CF)
4) Integrity (I)
5) Availability (A)
6) Compliance (C)
7) Reliability (R)

Nonetheless, the following gaps have been observed in the COBIT framework:

1) Lack of alignment of process areas with business strategy
2) A maturity model that is mainly a stand-alone analysis tool that provides only a very shallow analysis of the situation.
3) COBIT provides 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
4) Audit and Information Security reporting gaps that can lead to lack of information flow between upper management and implementation teams.

Table 1

Weaknesses in BSC & COBIT and potential mitigation solutions (Goldman & Ahuja, 2009)

#	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
1.2	A vast amount of metrics that can be used to assess the maturity of IT governance processes. 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
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. There are previous examples of SEI-CMM to COBIT mapping. Using a similar approach, a maturity model can be developed
1.4	Audit and Information Security reporting gaps	Using a cascading balanced scorecard approach would establish an information security reporting mechanism via KPIs, KGIs and CSFs while measuring maturity via SSE-CMM
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, control and evaluation mechanism	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 from conflicts
2.2	Terminates at the "Initiatives" level without indicating what processes need to be implemented	Create a mapping between COBIT processes and BSC initiatives
2.3	Lack of traceability to information security level	Use of COBIT control processes over appropriate process areas that are related to information security management
2.4	Audit and Information Security reporting gaps	Using a cascading balanced scorecard approach would establish an information security reporting mechanism via KPIs, KGIs and CSFs while measuring maturity via SSE-CMM

Findings

Using an integrated approach that combines BSC, COBIT and SSE-CMM, the gaps identified in Table 1 can be addressed and mitigated. Figure 20 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.

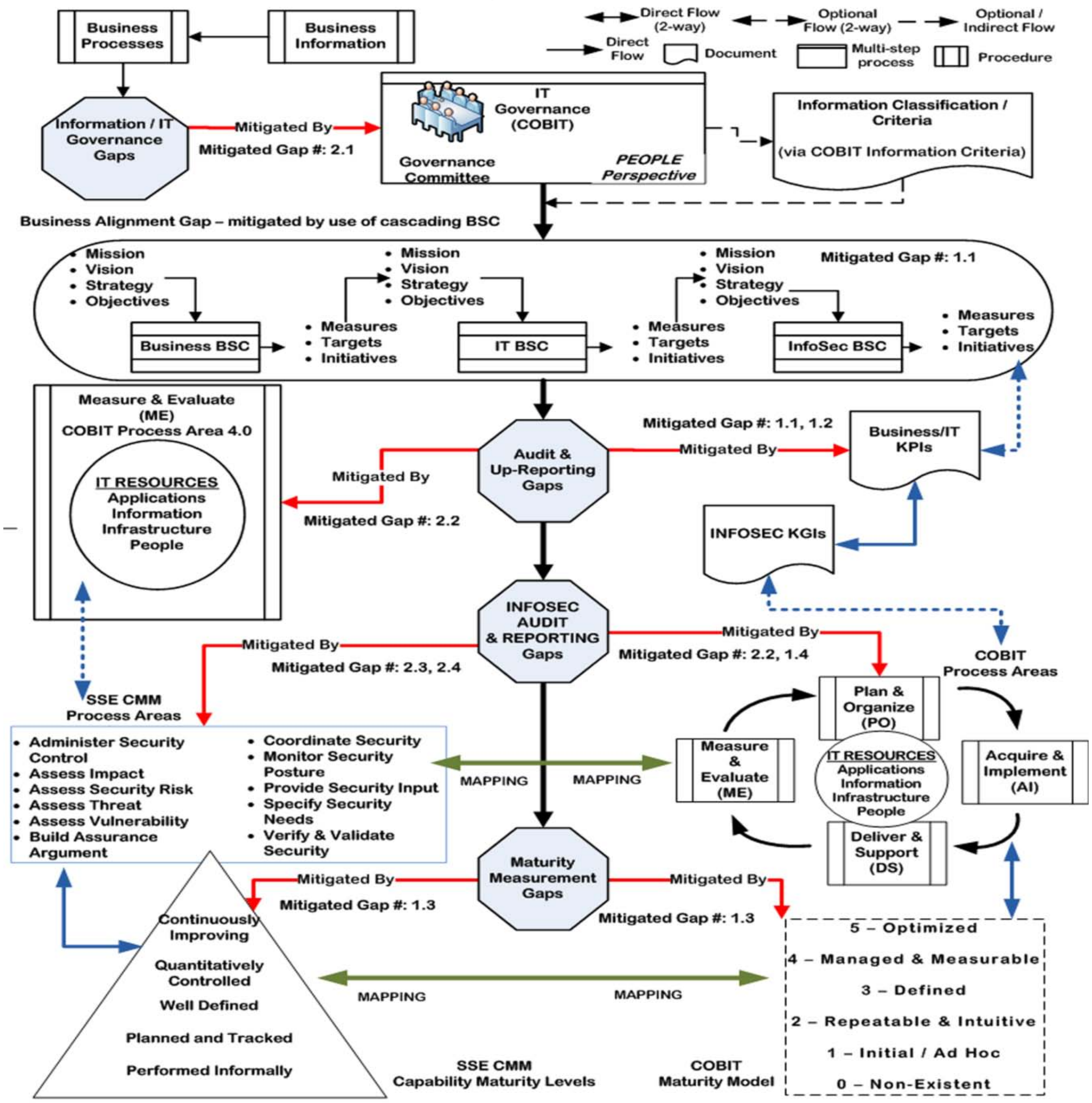

Figure 20. Mitigation of Gaps (Goldman & Ahuja, 2009)

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 (Mahnic & Zabkar, 2000), 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 21). 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

- 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.

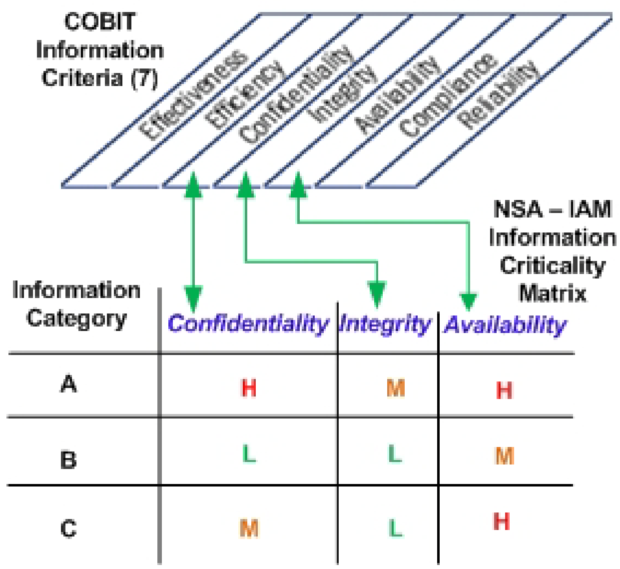

Figure 21. Information Classification Matrix & COBIT Information Criteria

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 22 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. 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).

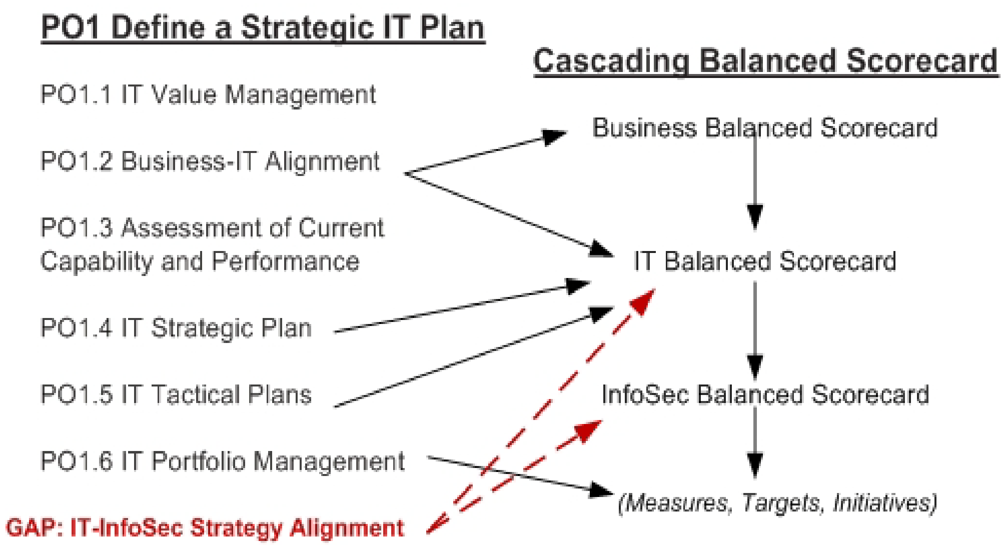

Figure 22. COBIT - Cascading BSC Mapping

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

SSE-CMM process areas must be mapped to appropriate COBIT process controls (Goldman & Ahuja, 2009). 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 23 below shows 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.

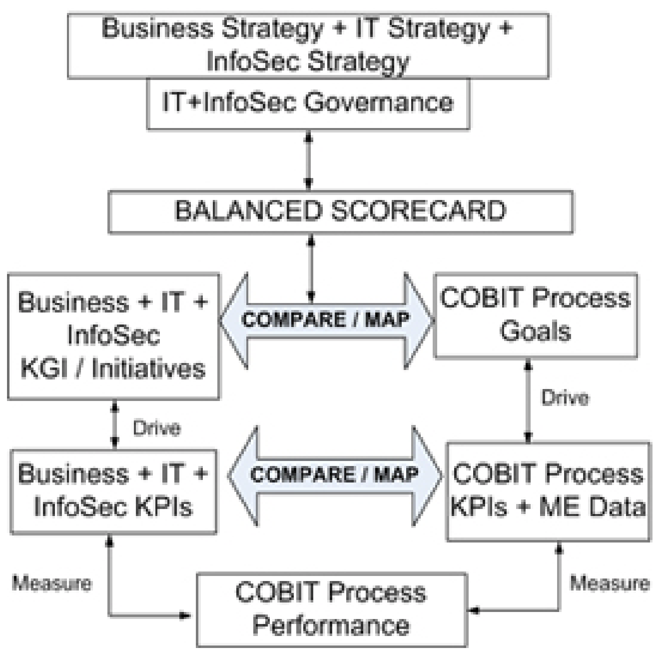

Figure 23. Cascading KPIs & KGIs for mitigation of Audit/Up-Reporting Gaps

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 by Goldman and Ahuja (2009), 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. 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 display in concise for simplification purposes, 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 the SSE-CMM manual. 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.

In order to provide a better understanding of the mapping in Table 2 below, the SSE-CMM process areas and base practices are shown in Table 3 below. These are the most frequently occurring process areas and base practices in the COBIT-SSECMM mappings.

Table 2

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

Table 3

SSE-CMM (v. 3.0) Process Areas & Base Practices

SSE-CMM (v. 3.0) Process Area	**Description**	**Base Practices**
PA 01	Administer Security Controls	1. Establish responsibilities and accountability for security controls and communicate them to everyone in the organization. 2. Manage the configuration of system security controls. 3. Manage security awareness, training, and education programs for all users and administrators. 4. Manage periodic maintenance and administration of security services and control mechanisms.
PA 02	Assess Impact	1. Identify, analyze, and prioritize operational, business, or mission capabilities leveraged by the system. 2. Identify and characterize the system assets that support the key operational capabilities or the security objectives of the system. 3. Select the impact metric to be used for this assessment 4. Identify the relationship between the selected metrics for this assessment and metric conversion factors if required 5. Identify and characterize impacts. 6. Monitor ongoing changes in the impacts.
PA 03	Assess Security Risk	1. Select the methods, techniques, and criteria by which security risks, for the system in a defined environment are analyzed, assessed, and compared. 2. Identify threat/vulnerability/impact triples (exposures). 3. Assess the risk associated with the occurrence of an exposure. 4. Assess the total uncertainty associated with the risk for the exposure. 5. Order risks by priority. 6. Monitor ongoing changes in the risk spectrum and changes to their characteristics.
PA 04	Assess Threat	1. Identify applicable threats arising from a natural source. 2. Identify applicable threats arising from man-made sources, either accidental or deliberate. 3. Identify appropriate units of measure, and applicable ranges, in a specified environment. 4. Assess capability and motivation of threat

		agent for threats arising from man -made sources. 5. Assess the likelihood of an occurrence of a threat event. 6. Monitor ongoing changes in the threat spectrum and changes to their characteristics.
PA 05	Assess Vulnerability	1. Select the methods, techniques, and criteria by which security system vulnerabilities in a defined environment are identified and characterized. 2. Identify system security vulnerabilities. 3. Gather data related to the properties of the vulnerabilities. 4. Assess the system vulnerability and aggregate vulnerabilities that result from specific vulnerabilities and combinations of specific vulnerabilities. 5. Monitor ongoing changes in the applicable vulnerabilities and changes to their characteristics.
PA 06	Build Assurance Argument	1. Identify the security assurance objectives. 2. Define a security assurance strategy to address all assurance objectives. 3. Identify and control security assurance evidence. 4. Perform analysis of security assurance evidence. 5. Provide a security assurance argument that demonstrates the customer's security needs are met.
PA 07	Coordinate Security	1. Define security engineering coordination objectives and relationships. 2. Identify coordination mechanisms for security engineering. 3. Facilitate security engineering coordination. 4. Use the identified mechanisms to coordinate decisions and recommendations related to security.
PA 08	Monitor Security Posture	1. Analyze event records to determine the cause of an event, how it proceeded, and likely future events. 2. Monitor changes in threats, vulnerabilities, impacts, risks, and the environment. 3. Identify security relevant incidents. 4. Monitor the performance and functional effectiveness of security safeguards. 5. Review the security posture of the system to identify necessary changes. 6. Manage the response to security relevant incidents. 7. Ensure that the artifacts related to security

		monitoring are suitably protected
PA 09	Provide Security Input	1. Work with designers, developers, and users to ensure that appropriate parties have a common understanding of security input needs. 2. Determine the security constraints and considerations needed to make informed engineering choices. 3. Identify alternative solutions to security related engineering problems. 4. Analyze and prioritize engineering alternatives using security constraints and considerations. 5. Provide security related guidance to the other engineering groups. 6. Provide security related guidance to operational system users and administrators.
PA 10	Specify Security Needs	1. Gain an understanding of the customer's security needs. 2. Identify the laws, policies, standards, external influences and constraints that govern the system. 3. Identify the purpose of the system in order to determine the security context. 4. Capture a high-level security oriented view of the system operation. 5. Capture high-level goals that define the security of the system. 6. Define a consistent set of statements, which define the protection to be implemented in the system. 7. Obtain agreement that the specified security requirements match the customer's needs.
PA 11	Verify and Validate Security	1. Identify the solution to be verified and validated. 2. Define the approach and level of rigor for verifying and validating each solution. 3. Verify that the solution implements the requirements associated with the previous level of abstraction. 4. Validate the solution by showing that it satisfies the needs associated with the previous level of abstraction, ultimately meeting the customer's operational security needs. 5. Capture the verification and validation results for the other engineering groups.

Conclusions

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.

	ITGI Product	Responsibility	Strategy	Acquisition	Performance	Conformance	Human Behaviour	Evaluate	Direct	Monitor
COBIT is increasingly being adopted globally as the **'de facto standard'** *control model.*	*Board Briefing on IT Governance, 2nd Edition*	√	√				√	√	√	√
	Unlocking Value: An Executive Primer on the Critical Role of IT Governance	√	√				√	√	√	√
	COBIT®	√	√	√	√	√	√	√	√	√
	Val IT™	√	√	√	√	√	√	√	√	√
Val IT was introduced to extend ITGI guidance into the area of IT-enabled investments.	*IT Governance Implementation Guide: Using COBIT® and Val IT, 2nd Edition*							√	√	√
	IT Assurance Guide: Using COBIT®				√	√		√		√
	COBIT® Quickstart™, 2nd Edition							√	√	
	Enterprise Value: Governance of IT Investments, Getting Started With Value Management							√		
The combination of Val IT and COBIT frameworks	*COBIT® Security Baseline™, 2nd Edition*	√						√	√	
	Enterprise Value: Governance of IT Investments, The Business Case			√	√			√	√	√

Figure 24. Organizational impact of a COBIT implementation (ITGI, 2008)

The strategic ISM framework proposed in this study may find direct applicability in the governance, risk and compliance (GRC) domain of business. As seen from Figure 24 above, COBIT is the de facto standard control model and covers several organizational areas like responsibility, evaluation, acquisition, conformance, strategy, etc. These areas are directly related to ISO 38500, which is a standard model for IT Governance. Thus, the applicability of the strategic framework is broader than just security management.

The success of the strategic ISM 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.

Discussion about risk management within the strategic ISM framework

In order to address "information security management" issues within an organization adequately, it is important to consider the organizational processes for risk management. During development of this framework, several concerns regarding "risk management" within the framework were addressed informally. However, an exclusive "risk management" process area cannot be effectively designed within the framework because organizational processes for risk management vary uniquely depending on several organizational factors. These organizational factors may include the following:

- size of the organization
- complexity of existent risk management practices
- level of adoption of COBIT within the organization
- organizational risk management maturity
- potential integration problems with existent risk management processes

COBIT prescribes risk management within the Plan & Organize (PO) domain. The process area PO 9 – Assess and Manage IT Risks, makes risk management an integral part of the COBIT framework but no methodology or standardized tool is recommended. This is because organizations may choose to implement COBIT processes using various approaches and specifying a standardized tool may not always result in the best outcome for a particular organization. Therefore, it may choose to implement a risk management approach using a tool that fits the requirements of the organization. For example, an organization may choose to use NIST 800-53 as a risk management guideline but other organizations may have requirements that are more specific and could choose to use NIST 800-33 or NIST 800-53.

Recommendations for future work

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. 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 (ISACA, 2009) 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 research is Business/IT/Information Security alignment. The extensive use of BSC in academic research and industry implementation provides quality literature and credibility. ValIT is a comparatively newer framework and does not possess a significantly large publication base.

Hence, recommendations for future work related to this research study include:

- implementation of the proposed ISM framework at a credible organization
- reporting the performance of the information security processes prior to and post implementation
- mapping of ValIT with this framework
- assessing the ROI (return on investment) from the implementation of the framework
- analyzing the effect of this framework on overall audit based activities and reporting performance levels

References

Ahn, H. (2001). Applying the Balanced Scorecard Concept: An Experience Report. *Long Range Planning*. 34(4), pp. 441-461.

Aitoro, J.R. (2008). OMB reports 60 percent increase in information security incidents. *Government Executive*. Retrieved February 1, 2009 from http://www.govexec.com/dailyfed/0308/030208a1.htm

AMR Research. (2008). The Governance, Risk Management, and Compliance Spending Report. Retrieved March 6, 2009 from http://www.amrresearch.com/

Balanced Scorecard Institute [BSCI]. (2009). About - Balanced Scorecard. Retrieved March 1, 2009 from http://www.balancedscorecard.org/BSCResources/AbouttheBalancedScorecard/tabid/55/Default.aspx

Business Software Alliance. (2003). Retrieved February 1, 2009 from http://www.bsa.org/country.aspx?sc_lang=en

Chapin, D.A., Akridge, S. (2005). How can security be measured? Information Systems Control Journal, Volume 2, 2005. Retrieved March 11, 2009 from http://www.isaca.org/Content/ContentGroups/Journal1/20058/jpdf052-how-can-security.pdf

Cobbold, I.M., Lawrie, G.J.G. (2002). The development of Balanced Scorecard as a Strategic Management Tool. 2GC Active Management Ltd. Retrieved October 18, 2008 from http://humanresources.co.za/free/Downloads/BSC.pdf

COBIT Mapping: Mapping SEI's CMM for Software with COBIT 4.0. (2007). IT Governance Institute. Retrieved December 7, 2008 from http://www.isaca.org/Template.cfm?Section=COBIT_Mapping1&Template=/ContentManagement/ContentDisplay.cfm&ContentID=27170

Computer Weekly. (2008). Heavy-handed security bypassed by employees, says research. Retrieved March 7, 2009 from http://www.computerweekly.com/Articles/2008/03/31/230054/heavy-handed-security-bypassed-by-employees-says-research.htm

Curtis, M.B., & Wu, F.H. (2000). The components of a comprehensive framework of internal control. *The CPA Journal*, 70(3):64-66.

Da Cruz, E. and Labuschagne, L. (2006). A new framework for bridging the gap between IT Service Management and IT Governance from a security perspective. *Academy of Information Technology at the University of Johannesburg.* Retrieved March 20, 2009 from http://icsa.cs.up.ac.za/issa/2005/Proceedings/Full/072_Article.pdf

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.*

Deloitte. (2009). Compliance Week and Deloitte Financial Advisory Services Survey. Retrieved March 4, 2009 from www.complianceweek.com/article/5171/survey-many-fearful-of-fraud-spike-in-2009

Elci, A., Ors, S., Preneel, B. (2008). Security of Information and Networks: Proceedings of the First International Conference on Security of Information and Networks (SIN 2007). Retrieved February 1, 2009 from http://books.google.com/books?id=zdsOFf9U8bkC&printsec=frontcover

Ernest, M. (2007). Adding value to the IT organization with the Component Business Model. *IBM Systems Journal*, 46(3), 387-389.

Ernst & Young. (2008). Global Information Security Survey. Retrieved March 5, 2009 from http://www.ey.com/Global/assets.nsf/UK/Global_Information_Security_Survey_2008/$file/EY_Global_Information_Security_Survey_2008.pdf

Evergreen Systems Inc. (2007). IT Governance Frameworks: ITIL and CobiT - Overhead or Strategic Weapon? Retrieved October 5, 2008 from www.itgi.org

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

Goldman, J.E. and Ahuja, S. (2009, June). The integrated use 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) held in conjunction with CAiSE'09 Conference.* Amsterdam: Springer Publication.

Grembergen, W. (2000). *The* Balanced Scorecard and IT Governance. *Information Systems Control Journal*. 2(1), pp. xxx.

Grembergen, W. & Haes, S. (2005). *COBIT's Management Guidelines Revisited: The KGIs/KPIs Cascade*. *IT Governance Institute Publication*, Volume 6. Retrieved October 6, 2008 from http://www.itgi.org/Template.cfm?Section=Home&CONTENTID=24398&TEMPLATE=/ContentManagement/ContentDisplay.cfm#f3

Grembergen, W. & Haes, S. (2005a). Measuring and Improving IT Governance through the Balanced Scorecard. *Information Systems Control Journal*, volume 2, 2005.

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.

IT Governance Global Status Report. (2008). IT Governance Institute. Retrieved March 1, 2009 from http://www.itgi.org/AMTemplate.cfm?Section=ITGI_Research_Publications&Template=/ContentManagement/ContentDisplay.cfm&ContentID=39735

IT Governance Institute. (2008). Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit. Retrieved February 18, 2009 from http://www.isaca.org/Template.cfm?Section=COBIT_Mapping1&Template=/ContentManagement/ContentDisplay.cfm&ContentID=45932

IT Governance Institute. (2007). COBIT 4.1 Handbook. Retrieved October 5, 2008 from www.itgi.org

IT Governance Institute. (2007a). *COBIT Mapping: Mapping SEI's CMM for Software with COBIT 4.0*. Retrieved December 7, 2008 from http://www.isaca.org/Template.cfm?Section=COBIT_Mapping1&Template=/ContentManagement/ContentDisplay.cfm&ContentID=27170

IT Governance Institute. (2007b). *Information Security Governance: Guidance for Information Security Managers*. Retrieved October 5, 2008 from www.itgi.org

ISACA. (2008). Information Security Governance: Guidance for Information Security Managers. Retrieved October 5, 2008 from www.itgi.org

ISACA. (2009). ValIT Framework 2.0. Retrieved July 15, 2009 from http://www.isaca.org/Template.cfm?Section=Val_IT4&Template=/ContentManagement/ContentDisplay.cfm&ContentID=39994

Kaplan, R. S. (1996). Using the Balanced Scorecard as a Strategic Management System. *Harvard Business Review*, 74, 75-76.

Kaplan, R. S. (2005). The Balanced Scorecard: Measures that Drive Performance. *Harvard Business Review*, 83(7), 172-173.

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

Lainhart IV, J. (2000). COBIT: A Methodology for Managing and Controlling Information and Information Technology Risks and Vulnerabilities. Journal of Information Systems, 14(1), 21. Retrieved October 17, 2008, from Military & Government Collection database.

Larsen, H. M., Pedersen, K. M., & Viborg Andersen, V. K. (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.*

Mahnic, V. & 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.

Mallette, D. (2005). IT Performance Improvement with COBIT and the SEI CMM. *Information Systems Audit and Control Association (ISACA)*. Retrieved December 7, 2008 from http://www.isaca.org/Template.cfm?Section=COBIT_Mapping1&Template=/ContentManagement/ContentDisplay.cfm&ContentID=25094

Malina, A.M., Selto, F. H. (2001). Communicating and Controlling Strategy: An Empirical Study of the Effectiveness of the Balanced Scorecard Approach. *Journal of Management Accounting Research.* Retrieved October 18, 2008 from http://ssrn.com/abstract=278939 or DOI: 10.2139/ssrn.278939

Martinsons, M. (1999). The balanced scorecard: a foundation for the strategic management of information systems. *Decision Support Systems*, 25(1), 71-74.

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

Microsoft (2007). Balanced Scorecard for Information Security Introduction. *Microsoft TechNet – Security TechCenter.* Retrieved April 5, 2009 from http://technet.microsoft.com/en-us/library/bb821240.aspx

Niven, R.P. (2006). Balanced Scorecard Step-by-Step: Maximizing Performance and Maintaining Results. Edition 2. (pp. 216-218).

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.

NSA Infosec Assessment Methodology and Infosec Evaluation Methodology (NSA IAM/IEM) available at: http://www.securityhorizon.com/resources.php

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.

Pironti, J.P. (2006). Information Security Governance: Motivations, Benefits and Outcomes. *Information Systems Control Journal.* Volume 4.

PriceWaterhouseCoopers. (2006). IT governance survey 2006. Retrieved March 7, 2009 from http://www.pwc.com/Extweb/pwcpublications.nsf/docid/D3E2997D370F3C648025713300511A01

Privacy Rights Clearinghouse. (2009). Retrieved February 5, 2009 from http://www.privacyrights.org/ar/ChronDataBreaches.htm#2009

Remenyi, D. (2005). Centralization issues in IT governance: the role and responsibilities of the IT control officer from a European perspective. *Proceedings of the 12th European Conference on IT Evaluation.* pp.96

Ridley, G., et al. (2004). COBIT and its utilization: A framework from the literature. *Proceedings of the 37th Hawaii International Conference on System Sciences.*

Rigby, D. (2009). Management Tools and Trends 2007. Bain & Company Publication. Retrieved March 5, 2009 from http://www.bain.com/management_tools/tools_balanced.asp?groupCode=2

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.* Retrieved October 18, 2008 from http://www.symantec.com/ciodigest/articles/200704/old_school_cios_versus_cobit.html

Robinson, N. (2005). IT excellence starts with governance. *Journal of Investment Compliance.* 6(3), pp. 45-49.

Rohm, H., Halbach, L. (2005). Developing and Using Balanced Scorecard Performance Systems. *The Balanced Scorecard Institute*. Retrieved February 1, 2009 from http://www.google.com/url?sa=U&start=1&q=http://www.performancesoft.com/pdfs/wp/

balancingact.pdf&ei=AwqdSfXyD4S4Mbq0qZoF&usg=AFQjCNFGP1q8vp_MJ4X3D_0898Dj-Ufm7Q

Rouyet-Ruiz, J. (2008). COBIT as a Tool for IT Governance: between Auditing and IT Governance. *The European Journal for the Informatics Professional*. Vol. IX, issue No. 1, February 2008. Retrieved October 17, 2008 from http://upgrade-cepis.net/issues/2008/1/upg9-1Rouyet.pdf

Schlarman, S. (2007). Selecting an IT Control Framework. EDPACS, 35(2), 11-17. Retrieved October 17, 2008, from ABI/INFORM Global database. (Document ID: 1253218061).

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

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. Retrieved October 18, 2008 from http://www.ee.kth.se/php/modules/publications/reports/2007/IR-EE-ICS_2007_026.pdf

Sipior, J.C., Ward, W.T. (2008). A Framework for Information Security Management Based on Guiding Standards: A United States Perspective. *Issues in Informing Science and Information Technology, Vol. 5*.

Society for Information Management. (2008). Retrieved February 5, 2009 from http://www.stevensnewsservice.com/pr/pr1206

SSE-CMM.org. (2009). How secure is SSE-CMM? Retrieved March 5, 2009 from http://www.secure-software-engineering.com/2008/02/19/how-secure-is-sse-cmm/

The Balanced Scorecard Institute. (2008). http://www.balancedscorecard.org/

Turner, M.J., Oltsik, J., McKnight, J. (2008). ISO, ITIL and COBIT triple play fosters optimal security management execution. *SC Magazine Awards 2009 - USA*. Retrieved February 1, 2009 from http://www.scmagazineus.com/ISO-ITIL-and-COBIT-triple-play-fosters-optimal-security-management-execution/article/108620/

Von Solms, B. (2001). Corporate Governance and Information Security. *Computers & Security*, 20(3), pp. 215-218.

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

Wang, C., Wulf, W.A. (1997). Towards a framework for security management. *NIST NISSC Conference Proceedings*. Retrieved March 11, 2009 from http://csrc.nist.gov/nissc/1997/proceedings/522.pdf

Weill, P. & Ross, J.W. (2004). IT Governance: How top performers manage IT decision rights for superior results. *Harvard Business School Press*, Boston, Massachusetts.

Appendix A – Cascading balanced scorecard example

Mission

To improve the health of patients and community through innovation and excellence in care, education, research and service.

Vision

To be an acknowledged leader in quality: clinical care, education and research. Excellence is measured by objective evidence and established best practices. Exemplary levels of respect and dignity are given to patients and their families, while professionalism and collegiality mark relationships among all employees and physicians.

Core Functional Area / BSC Perspectives	**Organizational Values**
1. Service Line Development 1. Increase the capacity of existing hospitals 2. Develop key clinical service lines 3. Develop Ambulatory Care/Outreach tactics 4. Land-bank for future growth	o A patient's total care, including mind, body and spirit o Quality of care and respect for life o Excellence in research
2. Medical Education 1. Incremental enhancement and growth of academics consistent with a 'Community Teaching' hospital 2. Physician Alignment: Develop physician capacity to meet needs both in sufficient numbers and clinical talent. 3. Seek creative ways to align with the medical community.	o Excellence in education for health care providers o Leadership in health promotion and wellness o Excellence in research
3. Operations & Finance 1. Clinical Quality 2. Customer Service 3. Patient Privacy & Security 4. Employee Satisfaction 5. Financial Performance 6. Streamline capabilities and increase capacity to generate the cash flow to support strategy	o Charity, equality and justice in health care o Quality of care and respect for life o An internal community of mutual trust and respect o Excellence in research
4. Technology 1. Clinical Care Technology 2. Data and IT Management 3. Patient Management 4. Electronic Medical Record (EMR) 5. Biometric authentication 6. Point-of-care technologies 7. Information Warehousing	o Leadership in health promotion and wellness o A patient's total care, including mind, body and spirit o Quality of care and respect for life

Table 4: Core Functional Areas - Business BSC Perspectives

Business Balanced Scorecard Pyramid

Key Strategies:

- S1: Develop Clinical Services at medical center and extension hospitals with focus on specialized services
- S2: Medical Education programs for workforce development
- S3: Streamline operations and increase financial capabilities
- S4: Strategic use of technology to achieve organizational goals

Strategy	Objectives	Detailed Objectives	Perspective
S1	S1-O1	Increase hospital capabilities and capacity	Service Line Development
	S1-O2	Develop clinical service lines	
	S1-O3	Ambulatory care / Outreach Programs	
	S1-O4	Develop for future extension	
S2	S2-O1	Physician alignment	Medical Education
	S2-O2	Community alignment	
	S2-O3	Develop teaching and research programs	
S3	S3-O1	Increase and streamline financial capabilities	Operations & Finance
	S3-O2	Improve clinical quality / patient privacy	
	S3-O3	Improve employee satisfaction	
	S3-O4	Improve customer service / satisfaction	
S4	S4-O1	Upgrade clinical care technology	Technology
	S4-O2	Support core clinical functions	
	S4-O3	Enhance patient data management	
	S4-O4	Universal accessibility	

Table 5: Objectives mapped to strategy

Perspective	Objective Detail	Measure	Measurement Details
Technology	Upgrade clinical care technology	S4-O1-M1 S4-O1-M2	% Automated clinical care tasks % Users of eHealth applications
	Support core clinical functions	S4-O2-M1 S4-O2-M2 S4-O2-M3	% increase in process automation % of technology enable requests % automated reporting / audit
	Patient data management	S4-O3-M1 S4-O3-M2 S4-O3-M3	% data availability # of transaction errors % electronic data
	Universal accessibility	S4-O4-M1 S4-O4-M2 S4-O4-M3	% systems using single sign-on % universal applications % online user base

Table 6: Measurements mapped to objectives

Perspective	Objective Detail	Target	Measurement Details	Target
Technology	Upgrade clinical care technology	S4-O1-M1-T1 S4-O1-M2-T1	% Automated clinical care tasks % Users of eHealth applications	70% 75%
	Support core clinical functions	S4-O2-M1-T1 S4-O2-M2-T1 S4-O2-M3-T1	% increase in process automation % of technology enable requests % automated reporting / audit	50% 50% 75%
	Patient data management	S4-O3-M1-T1 S4-O3-M2-T1 S4-O3-M3-T1	% data availability # of transaction errors % electronic data mgmt.	99.5% < 10/mth 60%
	Universal accessibility	S4-O4-M1-T1 S4-O4-M2-T1 S4-O4-M3-T1	% systems using single sign-on % universal applications % online user base	80% 65% 85%

Table 7: Fixing targets for future

Initiative	Measurement Details	Target	Initiatives
S4-O1-M1-T1-I1	% Automated clinical care tasks	70%	Deployment of point-of-care devices
S4-O1-M2-T1-I1	% Users of eHealth applications	75%	Development of eHealth programs
S4-O2-M1-T1-I1	% increase in process automation	50%	Implement process training programs and tools
S4-O2-M2-T1-I1	% of technology enable requests	50%	Deploy new Hospital Information System modules
S4-O2-M3-T1-I1	% automated reporting / audit	75%	Deploy enterprise software for audit and reporting
S4-O3-M1-T1-I1	% data availability	99.5%	Upgrade network and system infrastructure
S4-O3-M2-T1-I1	# of transaction errors	< 10/mth	Improve information / data services
S4-O3-M3-T1-I1	% electronic data mgmt.	60%	Conversion of paper records into e-records
S4-O4-M1-T1-I1	% systems using single sign-on	80%	Enterprise single sign-on solution
S4-O4-M2-T1-I1	% universal applications	65%	Deploy remote-access solutions and web services
S4-O4-M3-T1-I1	% online user base	85%	Promote online scheduling, EMR, knowledge base

Table 8: Organization-level initiatives

IT Balanced Scorecard

Information Technology Services collaborates with core functional areas in the organization regarding the development and implementation of technology-based solutions. The identified technology strategies throughout the organization mapped to the overall functional areas are depicted in **Table 9** below:

- S1: Lead the development of Clinical Services at medical center and extension hospitals
- S2: Develop tools and techniques to assist in Medical Education programs for workforce development
- S3: Provide strategic technology resources to streamline operations and cut operation costs
- S4: Strategic use of technology to achieve organizational goals

Strategy	Objectives	Detailed Objectives	Perspective
S1	S1-O1	Leverage IT to improve clinical outcomes	Service Line Development
	S1-O2	Develop clinical informatics practices	
	S1-O3	Patient lifecycle automation	
	S1-O4	Provide Clinical and Physician support	
S2	S2-O1	Develop training and support tools for physician alignment	Medical Education
	S2-O2	Develop training and support tools for community alignment	
	S2-O3	Develop web-based teaching and research tools	
S3	S3-O1	Tools for IT budget and administration	Operations & Finance
	S3-O2	IT Governance	
	S3-O3	Improve employee satisfaction	
	S3-O4	Improve customer service / satisfaction	
S4	S4-O1	Deployment of point-of-care devices	Technology
	S4-O2	Deploy new Hospital Information System modules	
	S4-O3	Improve information / data services	
	S4-O4	Improve patient security and privacy services	

Table 9: IT BSC strategies mapped to Business BSC perspectives

For simplification purposes, only ONE PERSPECTIVE shall be illustrated further:

Perspective	Objective Detail	Measure	Measurement Details
Service Line Development	Leverage IT to improve clinical outcomes	S1-O1-M1 S1-O1-M2	% Physician CPOE # Physician Portal Usage (Knowledge)
	Develop clinical informatics practices	S1-O2-M1 S1-O2-M2	% centralized patient records % online scheduling
	Patient lifecycle automation	S1-O3-M1 S1-O3-M2	% patients in EMR system % patients with automated charts/ billing
	Provide Clinical and Physician support	S1-O4-M1 S1-O4-M2 S1-O4-M3	# Physician Calls Addressed via Site Visit # Remote calls # Issues resolved online / phone

Table 10: IT Measurements

Perspective	Objective Detail	Target	Measurement Details	Target
Service Line Development	Leverage IT to improve clinical outcomes	S1-O1-M1-T1 S1-O1-M2-T1	% Physician CPOE # Physician Portal Usage (Knowledge)	70% 75%
	Develop clinical informatics practices	S1-O2-M1-T1 S1-O2-M2-T1	% centralized patient records % online scheduling	50% 50%
	Patient lifecycle automation	S1-O3-M1-T1 S1-O3-M2-T1	% patients in EMR system % patients with automated charts/ billing	75% 50%
	Provide Clinical and Physician support	S1-O4-M1-T1 S1-O4-M2-T1 S1-O4-M3-T1	# Physician Calls Addressed via Site Visit # Remote calls resolved # Issues resolved online / phone	<10/day <10/day <10/day

Table 11: Targets

Initiative	Measurement Details	Target	Initiatives
S1-O1-M1-T1-I1 S1-O1-M2-T1-I1	% Physician CPOE # Physician Portal Usage (Knowledge)	70% 75%	CPOE Module integration with Hospital Info. Sys. Enable & Integrate Physician Portal online
S1-O2-M1-T1-I1 S1-O2-M2-T1-I1	% centralized patient records % online scheduling	50% 50%	Implement EMR Online registration and scheduling system
S1-O3-M1-T1-I1 S1-O3-M2-T1-I1	% patients in EMR system % patients with automated charts/ billing	75% 50%	Implement EMR + Clinical Mgmt. System Implement and Integrate Patient chart with billing module
S1-O4-M1-T1-I1 S1-O4-M2-T1-I1 S1-O4-M3-T1-I1	# Physician Calls Addressed via Site Visit # Remote calls resolved # Issues resolved online / phone	<10/day <10/day <10/day	Online Ticketing and Issue Mgmt. System Remote connectivity software installation Support call center operations improvement

Table 12: IT Organizational Level Initiatives

Information Security Balanced Scorecard

In order to maintain the traceability of the security strategy, we shall use a limited set of parameters from the COBIT recommendations. We shall first map some of the higher-level COBIT parameters to HIPAA controls and then try to align these with the results of the IT Balanced scorecard. The outcome of this exercise will be an Information Security Balanced Scorecard that will use the organizational-level objectives and initiatives of the IT Balanced scorecard and specify specific application to information security areas. The goal is to try and perfectly align information technology initiatives to the information security initiatives.

HIPAA Drivers	COBIT Mapping {PO+AI+DS+ME}	IT + InfoSec BSC Mapping
1. Information System Activity Review	o Monitoring and Reporting o Problem Tracking and Audit Trail o Violations o Security Activity Reports	Service Line Development o CPOE Integration (S1) o EMR System
2. Security Awareness and Training	o Security Reminders o Protection from Malicious Software o Log-in Monitoring o Password Management	Medical Education o Online portal access (S2) o Educational Modules
3. Facility Access Controls	o Contingency Operations o Facility Security Plan o Access Control and Validation Procedures o Maintenance Records	Operations (S3)
4. Information Access Management	o Identification, Authentication and Access Control o Security of Online Access to Data o User Account Management	All Technology components (S4)

Table 13: HIPAA-COBIT-InfoSec BSC mapping

Strategy-Objective	**Objective Detail**	**Measures**	**Measurement Details**
S1 Secure CPOE Integration	Monitor & Report	S1-O1-M1	# of security reports generated per day
	Problem Tracking	S1-O2-M1	% of reported security issues traced vs. unresolved
	Violations	S1-O3-M1	% of security violations detected per day

Table 14: COBIT Security Objectives Mapping

Strategy-Objective	**Objective Detail**	**Targets**	**Measurement Details**	**Target Details**
S1-O1 Secure CPOE Integration	Monitor & Report	S1-O1-M1-T1	% of security CPOE events generated per day vs. total CPOE events	< 10%
	Problem Tracking	S1-O2-M1-T1	% of reported security issues traced vs. unresolved	90%
	Violations	S1-O3-M1-T1	% of security violations detected per day	100%

Table 15: Targets

Initiative	**Measurement Details**	**Target**	**Initiatives**
S1-O1-M1-T1-I1 S1-O1-M1-T1-I2 S1-O1-M1-T1-I3	% of security CPOE events generated per day vs. total CPOE events	< 10%	Enhance CPOE security evaluation process Increasing physician awareness by providing additional training Increasing application awareness by providing additional training to configuration mgmt. teams
S1-O2-M1-T1-I1	% of reported security issues traced vs. unresolved	90%	Historical tracking tools, training for current staff, ticketing and reporting system
S1-O3-M1-T1-I1	% of security violations detected per day	100%	IDS / IPS

Table 16: Initiatives