Concordia University College of Alberta

Master of Information Systems Security Management (MISSM) Program

7128 Ada Boulevard, Edmonton, AB

Canada T5B 4E4

Systematic Method of Achieving Sarbanes-Oxley (SOX) Compliance By Harmonizing COBIT, ITIL and ISO 27002/17799

by

SACHEDINA, Nisha

A research paper submitted in partial fulfillment of the requirements for the degree of

Master of Information Systems Security Management

Date: April 2008

Research advisors:

Pavol Zavarsky, Director of Research and Associate Professor, MISSM

Ron Ruhl, Director and Associate Professor, MISSM

Systematic Method of Achieving Sarbanes-Oxley (SOX) Compliance By Harmonizing COBIT, ITIL and ISO 27002/17799

by

SACHEDINA, Nisha

Research advisors:

Pavol Zavarsky, Director of Research and Associate Professor, MISSM

Ron Ruhl, Director and Associate Professor, MISSM

Reviews Committee:

Andy Igonor, Assistant Professor, MISSM
Dale Lindskog, Assistant Professor, MISSM
Ron Ruhl, Assistant Professor, MISSM
Pavol Zavarsky, Associate Professor, MISSM

Date: April 2008

The author acknowledges the significant contributions to the work by the Research Advisors and the Review Committee Members and gives the right to Concordia Univeristy College of Alberta to reproduce the work for the Concordia Library, Concordia Websites, and Concordia MISSM classes.

Concordia University College of Alberta
Information Systems Security Management
7128 Ada Boulevard, Edmonton, AB
Canada T5B 4E4

Systematic method of achieving Sarbanes-Oxley (SOX) compliance by harmonizing Cobit, ITIL and ISO 27002/17799

Nisha Sachedina

Master of Information Systems Security Management

Research advisors:
Pavol Zavarsky, Director of Research and Associate Professor, MISSM
Ron Ruhl, Director and Associate Professor, MISSM

April 2008

Table of Contents

Abstract

The financial industry internationally is under a lot of scrutiny to provide an accurate reporting of their financial statements. Multiple frameworks exist but there are no guidelines for implementation. The guidelines that exist are ambiguous and hard to follow. A robust, compliance process is required that will move organizations towards accurate, high quality financial statements.
This paper demonstrates how multiple frameworks can be harmonized to meet a subset of the Sarbanes-Oxley (SOX) legislative requirements. It also provides a methodology for planning, implementing, evaluating and maintaining a defined level of IT Control environment.

1 Introduction

Since 2002, corporations in the United States have been struggling to comply with section 404, of the Sarbanes-Oxley Act, "Management assessment of internal controls" [2]. Corporations within Canada are facing this challenge with a similar legislation referred to as Bill 198. Canada's equivalent to section 404 is Bill 198, the internal control Instrument 52-111 (CSOX) that was released on February 4, 2005 by Canadian Securities Administrator. The Internal Control Instrument will be phased in over 4 years, as follows:

Table1 - CSOX compliance requirement

Market Capitalization (as at June 30/05)	Effective years ending on or after
> $500 million	June 30, 2006
< $500 million but > $250 million	June 30, 2007
< $250 million but > $75 million	June 30, 2008
< $75 million	June 30, 2009

A similar legislation will be passed in Japan, known as J-SOX that comes into effect April 2008. [7}

To comply with the above legislative requirements, the corporations are turning to best practice frameworks such as:

- the Control Objectives for Information and related technology (COBIT) has become an internationally accepted standard for IT governance and Control.
- the IT infrastructure Library (ITIL) is being adopted across the world as the best practise framework in the provision of IT service. IT service management is divided into two main areas; IT service delivery and IT service support.
- ISO/IEC 27002 (formely ISO17799) provides best practice recommendations on information security for initiating, implementing or maintaining Information Security Management Systems (ISMS). Information security is defined within the standard in the context of the C-I-A triad.

Financial industry is required to provide an assertion that they have an adequate internal control environment. Organizations are struggling to meet this need, which is the direct cause of this research to derive an organization IT control framework. This paper will demonstrate how best practices from multiple frameworks for IT control (COBIT), IT service management (ITIL) and Information Security ISO/IEC 27002 (formely ISO17799) can be harmonized to provide the required IT control environment for the organization.

A systematic approach to developing an organization IT control framework can provide a means to achieving legislative compliance and also sustain an IT control environment as demonstrated by the following steps:

Plan

This involves gathering the requirements for the particular legislation that has to be enforced, in this case, SOX. Determine the impact of these requirements as they relate to the business processes. Map those requirements to the environments that are impacted. Harmonize the multiple frameworks to obtain IT control objectives to meet the requirements.

Do

Translate those requirements to the organization control objectives. Implement the policies and procedures to meet the control objectives. Build appropriate monitoring controls within the organization IT control framework.

Check

Ensure that the controls are functioning as designed and implemented. This can be done through implementing automated management controls or through regular audits.

Measurement

Verify the maturity levels of the controls that are implemented, are as desired or identify any adjustments that should be designed in the controls.

Correct

Implement the desired changes for the identified gaps by selecting new controls or adjusting current controls to meet the identified gaps.

Finally, the conclusion will sum up the findings and comments on the results of the methodology.

1.1 Sarbanes-Oxley act

The Sarbanes-Oxley act of 2002 was passed in the United States on July 30, 2002 as public law 107-204. This was done " to protect investors by improving the accuracy and reliability of corporate disclosures "[2].

One of the specific sections of the act is Section 404 which mandates that each US public company's annual report contain an internal control report that:

(1) states management's responsibility for establishing and maintaining an adequate internal control structure and procedures for financial reporting; and

(2) contains an assessment, as of the end of the company's most recent fiscal year, of the effectiveness of the company's internal control structure and procedures for financial reporting.

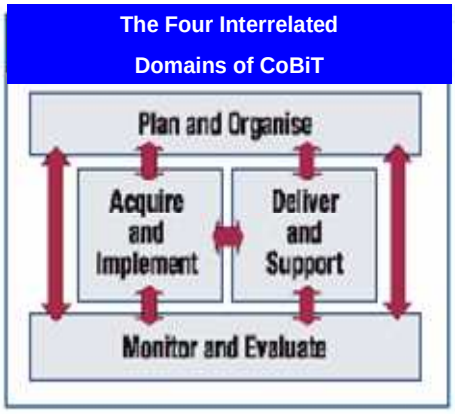
Section 404 requires the assessment of the effectiveness of the internal control structure of a company, which is directly dependent on the general computer control environment on which the financial application processing occurs.

Since financial applications are supported by IT systems, IT is considered a foundation of internal controls over financial reporting. SOX requires management to establish, evaluate and monitor the effectiveness of the controls over financial reporting that includes all the associated IT controls. The controls have to be tested to ensure that transactions processed through the systems are complete, accurate, valid and that the access to the systems is restricted and is appropriate. (this is often noted by the acronym CAVR)

1.2 COBIT Domains

The Commisssion of Sponsoring Organizations of Treadway Commission (COSO) has a framework which focuses on controls for financial processes and recognizes Control Objectives for Information and related Technology (COBIT), as an IT control framework that aligns with the COSO framework. The latest version of COBIT is COBIT 4.1, which is an open standard that is published by the IT Governance Institute (ITGI) and Information System Audit and Control Association (ISACA). With the management guidelines and revisions to the original framework, COBIT has become the internationally recognized IT control framework. Cobit framework consists of four interrelated domains, as shown in Figure 1. COBIT comprises of four domains, 34 IT processes and 318 detailed control objectives [3].

Figure 1 - COBIT domains. Reproduced with permission from [6]. Copyright 2007 IT Governance Institute



Mapping of subset of COBIT 4.0 control processes that satisfy the twelve IT control objectives for Sarbanes-Oxley are as follows:

Table 2 - IT Control Objectives for Sarbanes-Oxley. Reproduced with permission from [5]. Copyright 2006 IT Governance Institute.	***Cobit 4.0 Processes***
1. Acquire and maintain application software	A12
2. Acquire and maintain technology infrastructure	A13
3. Enable operations	A14
4. Install and accredit solutions and changes	A17
5. Manage Changes	A16
6. Define and manage service levels	DS1
7. Manage Third party services	DS2
8. Ensure System Security	DS5
9. Manage the configuration	DS9
10. Manage problems and incidents	DS8, DS10
11. Manage Data	DS11

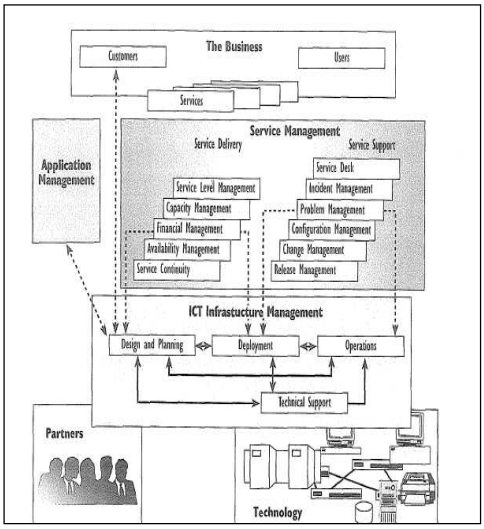
12. Manage the physical environment and operations	DS12, DS13

Three highlighted control objectives for SOX will be included in the detail below. The reason for selecting AI3, AI6, and DS5 is that these control objectives and processes are the most critical ones to provide the "CAVR" requirements for Sarbanes-Oxley.

1.3 ITIL activities

The Information Technology Infrastructure Library (ITIL) is a set of concepts and techniques for managing information technology (IT) infrastructure, development, and operations. It allows the organizations to manage service delivery by increasing system performance through reduced downtime and increased availability. ITIL was selected as the best practice for this paper as it complements COBIT. COBIT provides **what** objectives the processes should achieve, while ITIL describes **how** the processes should work to achieve those objectives. The following diagram obtained from the best practice, defines the system delivery and system support processes.

Figure 2: ICT Infrastructure Management Overview
Copyright 2006 OGC



Through standard set of centralized processes, cost of system support is reduced which in turn provides return on investment.

2 Systematic Method to Achieve compliance

2.1 Plan

The aim of the planning phase of the project is to define work scope to meet the compliance requirements for the Sarbanes-Oxley act. The best method to define scope for SOX requirements is to take a top down approach, as defined in figure 3.

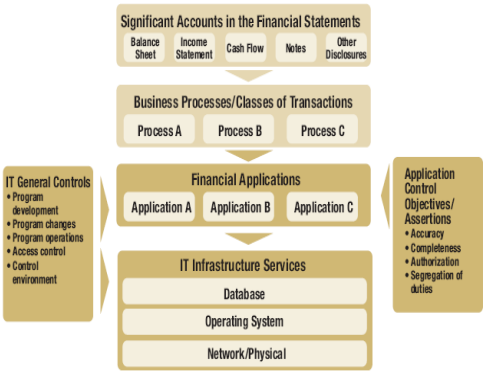
Since SOX requires reporting on Internal Control over Financial Reporting (ICFR), the scope of the environments impacted can be obtained by drilling down from the significant accounts in the financial statements. Once that is attained, the business processes that support the significant accounts are determined. These business processes are supported by the financial applications. SOX requirements need that the assertions have to be tested in the areas of CAVR:

- Completeness
- Accuracy
- Validation (authorization)
- Restricted access (segregation of duties)

This is mainly included in the application level testing, which will not be included as part of the scope of this paper.

This paper will mainly focus on the last layer, which is the IT General Controls, specifically the IT infrastructure services that support the financial applications. Lack of controls in this last layer can have a rippling impact and hence can misrepresent the numbers in the financial statements.

Figure 3 – Scoping the IT Control Project – Top Down
Reproduced with permission from [4].
Copyright 2006 IT Governance Institute



2.1.1 Define SOX requirements

Now that we have established the scope, we need to map the critical assets within the IT infrastructure services that support the financial applications. For SOX requirements, the key risks to those assets have to be identified and mitigated, to preserve the integrity of the information. The best method to achieving this is through an IT control framework, with well designed and implemented controls to mitigate and manage the identified risks.

2.1.2 Define related sample COBIT domains

COBIT has four main domains. Each of the domains consists of processes and within each process there are specific control objectives. COBIT standard will be used to develop an organization IT control framework, to mitigate the risks identified in section 2.1. COBIT will provide guidance for **what** we need to do.

As indicated in section 1.2, the three selected processes within the COBIT domains will be demonstrated further. These processes were selected as they are considered critical to preserve the integrity of the information, which is the key requirement for SOX.

Table 3 - IT Control Objectives for Sarbanes-Oxley. Reproduced with permission from [5]. Copyright 2006 IT Governance Institute.	***Cobit 4.0 Processes***
2. Acquire and maintain technology infrastructure	A13
5. Manage Changes	A16
8. Ensure System Security	DS5

AI3, Acquire and implement technology infrastructure provides control over acquiring and maintaining technology infrastructure that is standardized and supports the enterprise objectives. It consists of four control objectives:

1) Technology infrastructure acquisition plan
2) Infrastructure resource protection
3) Infrastructure maintenance
4) Feasibility test environment

These control objectives will be used to start to build the IT control framework, as identified in Appendix A. For the AI3 domain, we will use the first two objectives, Technology Infrastructure acquisition plan and infrastructure resource protection. Control objectives Infrastructure maintenance and feasibility test environment will be covered in the manage change process AI6.

AI6 manage changes is considered a critical control to minimise the likelihood of disruption, unauthorized alteration or error. All changes including emergency changes should be subject to a rigorous change management controls. Changes should also follow a defined system development life cycle. This process consists of four main control objectives:

1) Change standards and procedures to log all changes
2) Impact assessment, Prioritisation and Authorisation
3) Emergency changes
4) Change status tracking and reporting

2.1.3 Define the related sample ITIL activities

ITIL will provide us with **how** we implement the control objective that was selected using the COBIT standard.

As identified in Figure 2, the bottom layer of ITIL is the ICT infrastructure management. It consists of the following activities:

- design and planning
- deployment
- operation
- technical support

We use these activities within our control framework, to identify how we will meet the COBIT control objective.
For the second control objective, infrastructure resource protection, there are no associated ITIL activities. To fill this gap ISO/17799 standard will be used to provide the guidance of what activities need to be implemented.

Within ITIL service support, there are well defined activities for change management. Therefore we use the activities within service support, change management and we do not need to fill the gaps from ISO/17799.

2.1.4 Identify gaps in ITIL using ISO/ 17799

We use this standard to fill the gaps where there are deficiencies in the ITIL implementation. For infrastructure resource protection, we utilize the

ISO/17799 section 9.2 equipment security and complete the IT control framework.

2.2 Do

During the planning cycle, COBIT was used to identify what controls we need to implement. ITIL and ISO/17799 were utilized to identify how the processes can be implemented to meet the control objective. Within the do cycle, we are implementing the policies, procedures and standards to meet the control objectives within our organization, as identified in appendix A. These objectives can be implemented through automated tools or manual controls.

During this phase we assign the roles and responsibilities to individuals to implement the control. We need to identify the people that are **responsible** for implementing the control and the Individuals who are owners of the control and are **accountable.** It is the responsibility of the person who is accountable, to ensure that the control is implemented and is functioning, to detect or prevent an error from occurring.

2.3 Check

During the check cycle, the processes that we implemented for the control objective are evaluated to see if the processes meet the control objective. The results are documented and any gaps are identified.

Section 404 of the Sarbanes-Oxley act requires the assessing of the operating effectiveness of the controls. This requires the validation of:

- how the control is designed and implemented
- if the control was implemented consistently
- who is responsible and accountable to ensure the control is functioning adequately to detect or prevent an error over a period of time.

The testing of controls can be done through:

- observation
- inquiry
- re-performance

To be able to conclude on the operating effectiveness of the control, adequate evidence is required. Therefore observation or inquiry alone does not constitute testing the effectiveness of the control. Based on the frequency of the control, observation and enquiry have to be supplemented with sampling. The selection of appropriate sample sizes and sample distributions are important components in the overall adequacy of SOX testing.

The samples should be selected based on the frequency of the control:

- annual – 1
- quarterly – 2
- Monthly – 2-5
- Weekly – 5-10
- Daily – 10-20
- Many times per day – 25

Results of the tests are evaluated and any control deficiencies are documented.

2.4 Measurement

Capability Maturity Model Integration (CMMI) is a Software Engineering Institute framework that provides five maturity levels that can be utilized in a continuous improvement process such as plan-do-check-correct cycle. COBIT 4.0 uses the CMMI levels to measure the maturity of the IT control process. These levels are identified in table 4, maturity model for internal control. When we first start to build an organization IT control framework, most of the controls will probably be at level 0, non-existent or level 1, initial and ad hoc. As we progress through the iterations of plan-do-check-correct cycle, for SOX compliance initiative, the aim should be to get to level 4, managed and measurable.

Table 4- Maturity Levels.
Reproduced with permission from [6].

	Maturity Level	Status of the Internal Control Environment
0	Non-existent	There is no recognition of the need for internal control. Control is not part of the organisation's culture or mission. There is a high risk of control deficiencies and incidents.
1	Initial/*ad hoc*	There is some recognition of the need for internal control. The approach to risk and control requirements is *ad hoc* and disorganised, without communication or monitoring. Deficiencies are not identified. Employees are not aware of their responsibilities.
2	Repeatable but intuitive	Controls are in place but are not documented. Their operation is dependent on knowledge and motivation of individuals. Effectiveness is not adequately evaluated. Many control weaknesses exist and are not adequately addressed; the impact can be severe. Management actions to resolve control issues are not prioritised or consistent. Employees may not be aware of their responsibilities.
3	Defined process	Controls are in place and are adequately documented. Operating effectiveness is evaluated on a periodic basis and there is an average number of issues. However, the evaluation process is not documented. While management is able to deal predictably with most control issues, some control weaknesses persist and impacts could still be severe. Employees are aware of their responsibilties for control.
4	Managed and measurable	There is an effective internal control and risk management environment. A formal, documented evaluation of controls occurs frequently. Many controls are automated and regularly reviewed. Management is likely to detect most control issues but not all issues are routinely identified. There is consistent follow-up to address identified control weaknesses. A limited, tactical use of technology is applied to automate controls.
5	Optimised	An enterprisewide risk and control programme provides continuous and effective control and risk issues resolution. Internal control and risk management are integrated with enterprise practices, supported with automated real-time monitoring with full accountability for control monitoring, risk management and compliance enforcement. Control evaluation is continuous, based on self-assessments and gap and root cause analyses. Employees are proactively involved in control improvements.

This can be achieved through work flow process, which automates the routing for series of steps required to complete the process. For example, for change management, all changes are initiated through a gate keeper using a tool. The change then flows through a series of steps (approver, developer, Quality assurance, implementer), before it can be applied to production. By using a workflow process and automating a control, significant efficiencies are achieved, as SOX compliance testing will focus only on exceptions and required sample size for testing an automated control, can be reduced to one.

Along with the control deficiencies, requirements to reach to next level of maturity should also be evaluated. This can then feed into the correct phase of the cycle.

2.5 Correct

Based on the control deficiencies identified and maturity level attained, required corrective actions are recommended. This may require:

- Documenting the control
- Implementing a new control
- Providing adequate evidence that the control is functioning over a period of time.

These recommendations are then evaluated in the next planning cycle.

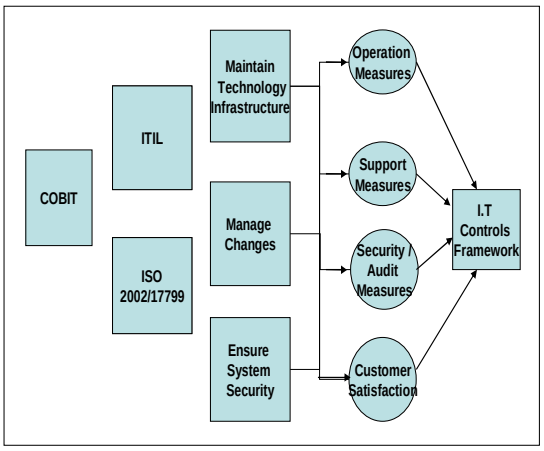
3 Conclusion

The aim of the Sarbanes-Oxley act was to improve the quality and reliability of financial reporting and maintain the confidence of the investors.
COBIT, ITIL and ISO/17799 can be used to guide the organizations to:

- help meet regulatory requirements for IT controls
- reduce complex IT-related risks
- optimize costs by standardizing controls
- assess how IT is performing
- enable effective governance of IT activities
- provide a management framework that helps staff understand what to do (policy, internal controls and defined practices)
- provide efficiency gains, fewer errors, increased trust from business partners and respect from regulators

However, in order to achieve the above benefits, it is important to note that the plan-do-check-correct cycle is a continuous process. As indicated in figure 4, different measures are used to improve and mature the processes and thereby improve the quality and reliability of IT controls. This will make the applications that feed the financial reporting more reliable and increase investor confidence.

Figure 4 – IT Control Framework Overview



4 Future Work

This research only demonstrates the methodology in achieving Sarbanes-Oxley compliance through creating an organization IT control framework. The academic community is positioned to further this research by completing the IT control framework for Sarbanes-Oxley compliance. There is growing need for SOX compliance internationally, as indicated in the article, "IT executives face J-SOX' compliance rules" [7]. Currently, there is no distinction in the SOX requirements for a small organization. Public Company Accounting Oversight Board (PCAOB) is working towards defining small company-specific requirements [8]. When this is available, differences in organization size can be explored and incorporated into the methodology. Additionally, this methodology can be utilized to create an IT control framework for other legislative compliance requirements or to define and sustain a control environment for Information Security.

5 Acknowledgments

I would like to thank my professors Pavol Zavarsky, Ron Ruhl, Dale Lindskog and Andy Igonor for their kind support, guidance and their precious help.

6 References

[1]Safford, George, (November 23, 2004) Control framework Misconceptions <http://itmanagement.earthweb.com/netsys/article.php/3439901>

[2] PUBLIC LAW 107–204—JULY 30, 2002 <http://www.ffiec.gov/ffiecinfobase/resources/audit/con-pl_107_204_116sta745-sarbanes_oxley.pdf>

[3] Fox, Christopher, Information Audit and Control Association, (2004) Sarbanes-Oxley considerations of a framework for financial reporting <https://www.isaca.org/Template.cfm?Section=Archives&Template=/MembersOnly.cfm&ContentID=10778>

[4] Fox, Chris, It governance Institute, (2004) IT control Objectives for Sarbanes-Oxley <http://www.isaca.org/TemplateRedirect.cfm?template=/MembersOnly.cfm&ContentID=33184>

[5] *The publication, IT Control Objectives for Sarbanes-Oxley: The Role of IT in the Design and Implementation of Internal Control Over Financial Reporting, 2nd Edition, <http://www.isaca.org/TemplateRedirect.cfm?template=/MembersOnly.cfm&ContentID=3277>*

[6} COBIT 4.1 excerpt executive summary <http://www.isaca.org/AMTemplate.cfm?Section=Downloads&Template=/ContentManagement/ContentDisplay.cfm&ContentID=34172>

[7] IT Executives face 'J-SOX' compliance rules <http://www.cio.co.uk/concern/compliance/news/index.cfm?articleid=1749>

[8] COSO small company guidance <http://www.coso.org/Publications/erm_sb/SB_Executive_Summary.pdf>

7 Appendix A IT control framework

	Plan			Do		Check				
	COBIT Objective	**ITIL activity**	**ISO17799 :2005**	**Organization control**	**Accountable/Responsible**	**Maturity**	**Test results**	**D = Designed I = Implemented E = Effective**		
								D	**I**	**E**
A3.1	Technology Infrastructure acquisition plan (Produce a plan for the acquisition, implementation and maintenance of the technological infrastructure that meets established business functional and technical requirements and is in accord with the organisation's technology direction.)	• design and planning • deployment • operation • technical support		• The organization has a documented acquisition and implementation plan • Procedures exist to ensure that infrastructure components are acquired and implemented as per the plan						
A3.2	Infrastructure resource protection (Implement internal control, security and auditability measures during configuration, integration and maintenance of hardware and infrastructural software to protect resources and ensure availability and integrity. Responsibilities for using sensitive infrastructure components should be clearly defined and understood by those who develop and integrate infrastructure components.	gap	• equipment hardening • equipment patch process • secure disposal of equipment • addressing security in third party agreements	• equipment hardening process • equipment patch management process • process to dispose equipment • if equipment is hosted at a service provider, security is addressed in vendor						

	Plan			Do		Check				
	COBIT Objective	**ITIL activity**	**ISO17799 :2005**	**Organization control**	**Accountable/Responsible**	**Maturity**	**Test results**	**D = Designed I = Implemented E = Effective**		
								D	**I**	**E**
	Their use should be monitored and evaluated.)			agreements						
AI6.1	Change standards and procedures to log all changes (Set up formal change management procedures to handle in a standardised manner all requests (including maintenance and patches) for changes to applications, procedures, processes, system and service parameters, and the underlying platforms.)	Service support, change management 8.5 activities		• documented change process with roles and responsibilities • all software and infrastructure changes are subject to change process						
AI6.2	Impact assessment, Prioritisation and Authorisation (Assess all requests for change in a structured way to determine the impact on the operational system and its functionality. Ensure that changes are categorised, prioritised and authorised.)	• Service Support, Change management, 8.5.6 impact and resource assessment • Service support, change management,		• change coordinator to prioritize and assess impact • Change advisory board for impact assessment and approval						
AI6.3	Emergency changes (Establish a process for defining, raising, testing, documenting, assessing and authorising emergency changes that do not follow the established change process.)	Service support		Included in AI6.1						

	Plan			Do		Check				
	COBIT Objective	**ITIL activity**	**ISO17799 :2005**	**Organization control**	**Accountable/Responsible**	**Maturity**	**Test results**	**D = Designed I = Implemented E = Effective**		
								D	**I**	**E**
AI6.4	Change status tracking and reporting (Establish a tracking and reporting system to document rejected changes, communicate the status of approved and in-process changes, and complete changes. Make certain that approved changes are implemented as planned)	Service support, configuration management, 7.9 relation to other processes		• segregation of environments • segregation of roles • configuration management database • change tracking tool						
DS5.1	Management of IT security (Manage IT security at the highest appropriate organisational level, so the management of security actions is in line with business requirements.)	gap	6.1.3 allocation of information security responsibilities	• document security responsibilities • allocate security responsibilities						
DS5.2	IT security plan (Translate business, risk and compliance requirements into an overall IT security plan, taking into consideration the IT infrastructure and the security culture. Ensure that the plan is implemented in security policies and procedures together with appropriate investments in services, personnel, software and hardware. Communicate security policies and procedures to stakeholders	Security management, fundamental of information security, 2.3.1.2 plan **gap**	• **5.1.2 Review of information security policy**	• approved information security policy, published and communicated to all employees and relevant third parties • policy review annually or when major changes occur						

	Plan			Do		Check				
	COBIT Objective	**ITIL activity**	**ISO17799 :2005**	**Organization control**	**Accountable/Responsible**	**Maturity**	**Test results**	**D = Designed I = Implemented E = Effective**		
								D	**I**	**E**
	and users)									
DS5.3	Identity management (Ensure that all users (internal, external and temporary) and their activity on IT systems (business application, IT environment, system operations, development and maintenance) are uniquely identifiable. Enable user identities via authentication mechanisms. Confirm that user access rights to systems and data are in line with defined and documented business needs and that job requirements are attached to user identities. Ensure that user access rights are requested by user management, approved by system owners and implemented by the security-responsible person. Maintain user identities and access rights in a central repository. Deploy cost-effective technical and procedural measures, and keep them current to establish user identification, implement authentication and enforce access rights.)	Security management, security management measures, 4.2.4 access control		• access control process, OS, network, application, third party • segregation of duties between requesting, approving, granting access • need to know and least privilege						
DS5.4	User account management (Address requesting, establishing, issuing,	Security management, security management measures, 4.2.4 access		Regular review of access privileges by application/data						

	Plan			Do		Check				
	COBIT Objective	**ITIL activity**	**ISO17799 :2005**	**Organization control**	**Accountable/Responsible**	**Maturity**	**Test results**	**D = Designed I = Implemented E = Effective**		
								D	**I**	**E**
	suspending, modifying and closing user accounts and related user privileges with a set of user account management procedures. Include an approval procedure outlining the data or system owner granting the access privileges. These procedures should apply for all users, including administrators (privileged users) and internal and external users, for normal and emergency cases. Rights and obligations relative to access to enterprise systems and information should be contractually arranged for all types of users. Perform regular management review of all accounts and related privileges.)	control		owners						
DS5.5	Security testing, surveillance and monitoring (Test and monitor the IT security implementation in a proactive way. IT security should be reaccredited in a timely manner to ensure that the approved enterprise's information security baseline is maintained. A logging and monitoring function will	Security management, security management measures, implement		• Accredit security • Log and monitor access • Protect log information						

	Plan			Do		Check				
	COBIT Objective	**ITIL activity**	**ISO17799 :2005**	**Organization control**	**Accountable/Responsible**	**Maturity**	**Test results**	**D = Designed I = Implemented E = Effective**		
								D	**I**	**E**
	enable the early prevention and/or detection and subsequent timely reporting of unusual and/or abnormal activities that may need to be addressed)									
DS5.6	Security Incident Definition (Clearly define and communicate the characteristics of potential security incidents so they can be properly classified and treated by the incident and problem management process)	Security management, 3.3.2 incident control/help desk		Incident response process						
DS5.7	Protection of Security Technology (Make security-related technology resistant to tampering, and do not disclose security documentation unnecessarily)	Security management, security management measures, 4.2 implementation		**Covered through other controls, not required.**						
DS5.8	Cryptographic key management (Determine that policies and procedures are in place to organise the generation, change, revocation, destruction, distribution, certification, storage, entry, use and archiving of cryptographic keys to ensure the protection of keys against modification and unauthorised	**Control not required for SOX**								

	Plan			Do		Check				
	COBIT Objective	**ITIL activity**	**ISO17799 :2005**	**Organization control**	**Accountable/Responsible**	**Maturity**	**Test results**	**D = Designed I = Implemented E = Effective**		
								D	**I**	**E**
	disclosure)									
DS5.9	Malicious software prevention, detection, and correction (Put preventive, detective and corrective measures in place (especially up-to-date security patches and virus control) across the organisation to protect information systems and technology from malware (e.g., viruses, worms, spyware, spam))	Security management, security management measures, 4.2 implementation		• Anti-virus process, prevention, detection, correction • Desktop measures, user cannot disable						
DS5.10	Network Security (Use security techniques and related management procedures (e.g., firewalls, security appliances, network segmentation, intrusion detection) to authorise access and control information flows from and to networks)	Security management, security management measures, 4.2 implementation		**Covered under other controls**						
DS5.11	Exchange of sensitive data (Exchange sensitive transaction data only over a trusted path or medium with controls to provide authenticity of content, proof of submission, proof of receipt and non-repudiation of origin)	Security management, security management measures, 4.2 implementation		• Process for transmission of sensitive information						