TOWARDS A FRAMEWORK FOR BUILDING SECURITY OPERATION CENTERS

A thesis submitted in partial fulfillment of

the requirements for the degree of

MASTERS OF SCIENCE

of

RHODES UNIVERSITY

by

Pierre Conrad Jacobs

September 2014

Abstract

In this thesis a framework for Security Operation Centers (SOCs) is proposed. It was developed by utilising Systems Engineering best practices, combined with industry-accepted standards and frameworks, such as the TM Forum's eTOM framework, CoBIT, ITIL, and ISO/IEC 27002:2005.

This framework encompasses the design considerations, the operational considerations and the means to measure the effectiveness and efficiency of SOCs. The intent is to provide guidance to consumers on how to compare and measure the capabilities of SOCs provided by disparate service providers, and to provide service providers (internal and external) a framework to use when building and improving their offerings.

The importance of providing a consistent, measureable and guaranteed service to customers is becoming more important, as there is an increased focus on holistic management of security. This has in turn resulted in an increased number of both internal and managed service provider solutions.

While some frameworks exist for designing, building and operating specific security technologies used within SOCs, we did not find any comprehensive framework for designing, building and managing SOCs. Consequently, consumers of SOCs do not enjoy a constant experience from vendors, and may experience inconsistent services from geographically dispersed offerings provided by the same vendor.

Acknowledgements

My gratitude and appreciation to Dr Alapan Arnab for his patience and guidance during this research project. His insights and inputs were of great value.

To Prof Barry Irwin, thank you for your guidance and mentorship.

To my wife, Marna, thank you for your continuous support, understanding and assistance. Without her encouragement it would have been impossible to complete this study. To my two children, Connor and Caylie, who will only understand later, thank you.

Finally, thank you to Tinus Jansen van Rensburg, who constantly motivated me to become the best I could be.

Table of Contents

List of Figures

List of Tables

1 Introduction

There is currently an increase in Security Operations Center (SOC) service providers, as well as in the establishment of in-house SOCs as part of the drive of organisations to provide a holistic solution to the security challenges that they face (Shenk, 2011).

A SOC serves as a central repository for log and security events. These events are generated by the technical controls that are deployed to protect an Organisation's IT assets. A typical function fulfilled by the SOC is incident management and escalation, as well as assisting with mitigation and containment of threats that observed against a network.

A SOC is process driven, and is supported by processes, people and technology. Kelley and Moritz (2006) describes the functionality of a SOC as an organisation that:

> *"monitors and manages all aspects of enterprise security in real-time from a single, centralized location. It discovers and prioritizes events, determines risk level and which assets are affected, and recommends and can execute the appropriate remediation solution. It delivers detailed reports at the local and network levels, meeting both real-time management and audit requirements."*

A key business driver for building SOCs is that it fulfils part of the risk management strategy for infrastructure and services (Lemos, 2012). Consuming SOC services realises the following benefits (Cisco Systems, 2007).

- Better risk management for critical information assets;
- Business continuity by identifying and reacting to incidents;
- Avoidance of disruption to critical assets and services;
- Prevention of the loss or contamination of data;
- Protection against loss of transactions or delayed transactions;
- Avoidance of customer service disruptions; and
- Visibility of an organisation's security posture

The need for security monitoring is also expressed in various standards and best practices. These are summarised in Appendix B.

There are several benefits to consuming SOC services, such as allowing for rapid and speedy response times to incidents, as well as allowing organisations to recover from Distributed Denial of Service (DDoS) attacks, and complying with governance, legal and other requirements (Rothke, 2009). McAfee (2012) defines a SOC as:

> *"…responsible for monitoring, detecting, and isolating incidents and the management of the organization's security products, network devices, end-user devices, and systems. This function is performed seven days a week, 24 hours per day. The SOC is the primary location of the staff and the systems dedicated for this function."*

Anderson (2013) defines a SOC as an entity that is dedicated to detect, investigate and respond to log events triggered by security related correlation logic by utilising people, processes and technology. In summary, it can be said that the SOC serves as a central repository for log data and events from security technical controls and other critical asset data, as well as for people, processes and technology. This enables its main task of monitoring and responding to security incidents. From a technology perspective, this is achieved using a Security Incident and Event Management tool (SIEM).

Given the increase in attacks on the human element as well as the ease with which technical controls are being bypassed (Applegate, 2009; SANS Institute, 2011; Tenable Network

Security, 2012), a SOC with added capability such as integrated electronic or automated Governance, Risk and Compliance (GRC) services, can also assist with enforcing and monitoring of administrative controls such as security policies. It can furthermore offer advanced services such as anomaly detection to mitigate zero-day attacks and human error. These are services offered by next-generation SOCs, as stated by Hewlett-Packard (2013) and others (ATOS Research, 2010). However, a Security Operation Center is not a silver bullet: attacks will happen and, depending on the monitoring of technical security controls, these attacks and compromises will sometimes go unnoticed. To this effect, companies should consider to move their focus from threat protection and detection to threat resilience by building on a foundation of preparedness, and also places responsibility of risk on the whole of business, and not on IT Security alone (Durbin, 2012). In this context, the SOC could play a valuable role in assisting with containment and mitigation.

SOCs can be centralised or distributed, and can be in-house or outsourced. Outsourced SOC service providers are known as Managed Security Service Providers (MSSPs).

Security Operation Centers fulfil all the functions encompassed in the prevent-detect-respond-recover model across people, processes and technology as mentioned in the ISACA Life Cycle and Functional Dimension of Security Convergence (ISACA, 2006). As such, they play a significant role when it comes to the defence of an organisation's critical assets, as well as in assisting with compliance issues. Such centers furthermore allow organisations to respond to threats in a timely fashion (Wang, 2010). These are defined as a required service by a number of international and national regulations and standards such as PCI-DSS (PCI Security Standards Council, 2010), ISO/IEC 27001:2005 (ISO/IEC, 2009), ECT Act (South African Government, 2002), Sarbanes Oxley (United States Government, 2002) and others (Swift, 2010).

1.1 Problem Statement

It is the experience of the researcher that the majority of consumers of SOC services do not enjoy a constant experience from vendors, and even more so from geographically dispersed offerings from the same vendors.

The experience of the author with the building and improvement of Security Operation Centers, both for the South African government and the private sector, has illustrated the lack of a framework or best practice which could be followed or used to build or improve such centers. Such a framework would ensure consistent quality in the delivery of the end product, and a lack of a framework could explain the lack of consistent service experienced by internal and external customers alike. Current documentation also focuses on point technologies, rather than on a holistic security solution.

A review of available literature in this domain has confirmed this observation.

For example, vulnerability management frameworks such as the framework proposed by Ghedini (2009), the Qualys framework (Qualys, 2012), as well as Security Incident and Event Monitoring (SIEM) frameworks by Bidou (2004), provide guidance for specific technologies but do not provide a comprehensive SOC framework.

In the event of a distributed architecture, the quality of the SOC services and customer experience can differ vastly if these centers are deployed without any guidance or framework. This leaves inconsistent service delivery to, and experience by, customers. Furthermore, there may be differences in understanding between the provider and consumer of these services with respect to the scope of the services. In many cases, not following a framework when building a SOC and not defining its services could lead to a SOC that does not really provide the service it should, or that provides a watered down service. It could also lead to a false

sense of security, which in many cases could be more dangerous than an entity that knows it either has good security, or does not have good security.

The lack of such a framework also leads to differing standards, processes and procedures, and often lacks minimum requirements from providers of SOC services. A reference or framework for a system or service is important since it ensures its repeatability, reduces risk, assists with predictable budgeting, and provides for a consistent outcome under the defined circumstances. It is just as important to be able to measure the effectiveness of a service or system in order to ensure its success. Investigation and research has shown the lack of any classification or effectiveness measurement scheme or tool for SOC services.

A classification guide will allow SOCs as well as prospective clients the opportunity to measure themselves and to improve where necessary, and will supply consumers of SOC services with a reference as to the effectiveness of the service that they procure. Business requirements would drive the requirements for a SOC service. There would typically be regulatory frameworks mandating that IT Security technical controls as well as other controls be monitored to prove compliance to the regulatory frameworks. These could be acts and standards business has to adhere to, as well as internal regulatory frameworks. Business will mandate a requirement for monitoring and other security related services, and these will be fulfilled by a SOC. The functions a SOC has to fulfil will be determined by business requirements, which in turn are driven by internal and external regulatory frameworks.

However, in the case of a SOC being a MSSP, it will have to fulfil different requirements from different businesses. This is mostly a technology (SIEM) issue i.e. compliance reporting, storage of events, devices and types of devices monitored, and a process issue where incident management will have to be aligned with different businesses' incident management and change management systems and processes. It is not feasible to provide 50 different daily firewall reports to 50 different customers. This thesis strives to identify the SOC requirements and build a framework around that. There is definitely a reciprocal element between business and security, but this should follow logically. Incident management will be aligned with business requirements in the same way as monitoring requirements, and all other SOC services.

This study identifies the *what*. There *has* to be monitoring, or there *has* to be incident management as mandated by business and other requirements - that is the what. The *how* will differ from business to business and is not the subject of this work. In this study, the SOC is seen as a business, and the framework is developed to answer *what* a SOC should look like from a business, people and functional perspective.

The current problems that need to be addressed are:

- The lack of a comprehensive SOC framework to be used when designing, building and managing SOCs;
- The lack of a mechanism or model for measuring the effectiveness of SOCs;
- The lack of a mechanism or model for measuring the maturity of SOCs.

1.2 Research Objective

In summary of the problem, it can be said that there is no SOC framework in existence that allows for repeatable results when building, managing and improving SOCs. There is also no mechanism that allows for the measurement of the effectiveness of SOCs.

The objective of this research project is to develop a SOC framework. Once the framework has been developed, a method or tool needs to be developed to test and prove its effectiveness.

The associated research activities and research approach are as follows:

- The development of SOC functional, service and business requirements by applying Systems Engineering principles;
- The development of Measurements of Effectiveness (MoE's) for the functional, service and business requirements by applying Systems Engineering principles;
- The design of a framework using the Telecommunications Management Forum's (TMForum, 2013) eTOM process Frameworks (Milham, 2004), augmented by ISO/IEC 27001:2005 (ISO/IEC, 2009) CoBIT 4.1 (Adler, 2007a), ITILv3 (NoxGlobe, 2011), NIST (Northcutt, 2009) and SANS Critical Controls (SANS, 2013), and,
- The design of a SOC classification model using detailed technical requirements, MoE's and industry-accepted maturity models.

In order to achieve these goals, Systems Engineering (SE) principles will be used to determine the SOC functional requirements, the SOC service requirements and the SOC business requirements, inclusive of aspects relating to people. Measures of Effectiveness (MoE's) will be assigned to the requirements to enable the development of the framework, and the development of a classification model. This concept is illustrated in Figure 1-1.

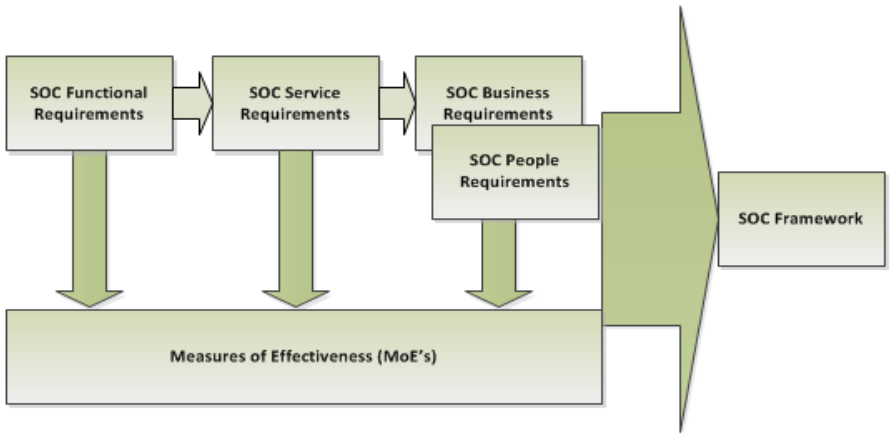

Figure 1-1: Collective Framework Development Tasks

The tasks are related and do not have to occur in sequence. The first three tasks need to be completed to serve as input to the classification scheme, and the last task (the framework) will utilise the output from the first three tasks to map back to the TM Forum framework.

The research problem statement and objectives are depicted in Figure 1-2.

1.3 Scope

In the study, the SOC is seen as a system. As such, SE principles will be used to determine the functional requirements. However, a SOC is more than just functional requirements, people requirements and technology requirements. Fundamentally, a SOC is a response to a business problem, and should also be seen as part of a business – when looking at SOCs from an internal perspective – or a fully-fledged business on its own when seen from a Managed Security Service Provider (MSSP) perspective. To this effect, suitable frameworks and standards will be identified and their use justified, as opposed to identifying all available

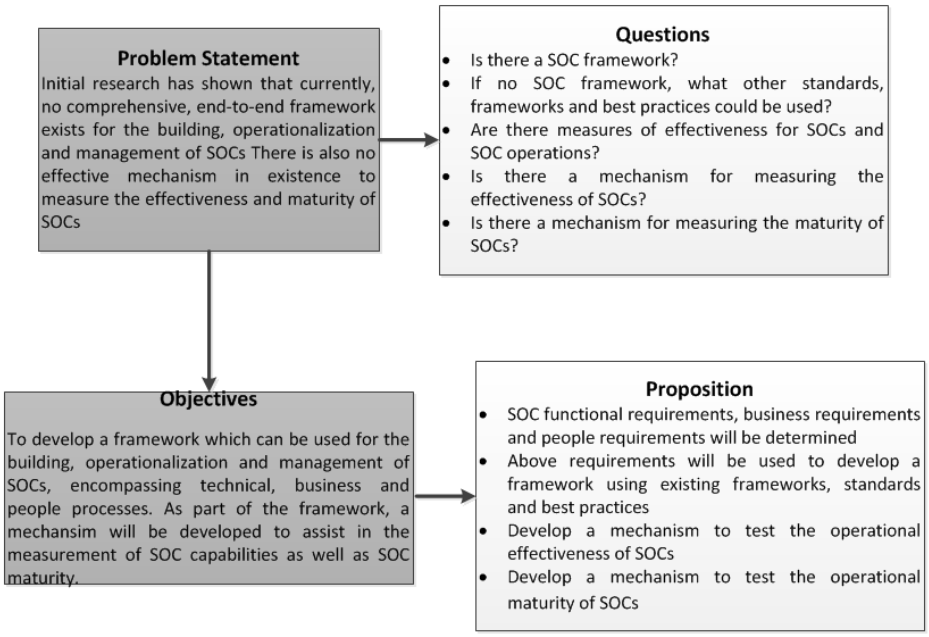

Figure 1-2: Problem statement and objectives

standards and frameworks, and motivating their exclusion. Technology aspects *do not* form part of the scope of this study, but one has to keep in mind that technology is used to deliver some of the functions of a SOC. Distinct and exact technologies enabling SOC functions will not be discussed. The following aspects form the scope of the study:

- SOC Functional requirements
- SOC People requirements
- SOC Business requirements

1.4 Type of Research

This study will comprise of the following research methodologies:

- Theory building research
  - The research will focus on the availability of SOC frameworks, as well as literature related to SOCs. This will be covered in section 2 of this document
- Theory testing research
  - In this section, existing SOC requirements will be analysed evaluated. This will provide a starting point for the determination of SOC functional, business and people requirements. In the absence of existing framework, industry best practices, standards and frameworks will be identified and analysed to assist with the development of the SOC framework.
- Theory application research
  - If the lack of a proper framework can be proved, the framework will be tested against expert reviewers since there will be no frameworks to measure the newly developed framework against.

1.5 Significance of the research

Given the importance of SOCs and the ease by which technical controls are being circumvented (Maitland & Thomas, 2012), as well as the myriad of attack vectors that are available, it is important to have a way to detect these attacks.

Organisations consume SOC services to enable them to better protect their Information Security (IT) assets, as well as to assist with compliance to legal and statutory requirements. Having a framework would ensure a uniform and repeatable model for building SOCs. Furthermore, a classification scheme would enable SOC owners to improve on their service, and would enable consumers to make an informed choice when selecting a provider.

1.6 Limitations and assumptions of the study

The limitation of the study is that it will cover only SOCs, and not Computer Security Incident Response Teams (CSIRTs), which may be considered to fulfil a specialised subset of the functionalities of a SOC. The research itself is limited insofar as limited material on SOC frameworks exits.

1.7 Document Structure

The remainder of this document is organised as follows:

Chapter 2 – Literature Review: The literature review investigates related work.

Chapter 3 – SOC Requirements Analysis: The SOC requirements analysis analyses the functional, high-level technical and detailed technical requirements. Measures of Effectiveness are derived from these.

Chapter 4 – SOC Business Requirements: The SOC business requirements are determined, inclusive of people requirements.

Chapter 5 – SOC Maturity and Effectiveness Measurement: A model is proposed to measure the effectiveness of SOCs requirements.

Chapter 6 – Verification: An analysis of existing national and international SOCs will be done against the framework. Completeness of the framework will be proved, and review from industry experts will be obtained regarding the applicability of the framework, as well as its completeness.

Chapter 7 – Conclusion: The study is concluded**,** and findings are made regarding the achievement of the objectives, as well as the relevance of the framework and classification tool.

A list of Abbreviations can be found in Appendix A.

2 Literature Survey

2.1 Introduction

The purpose of this chapter is to identify information related to Security Operation Center frameworks. This section identifies resources that are relevant to Security Operation Center frameworks, classification guidelines and maturity levels, and provides a description and critical evaluation of each relevant resource.

After having done extensive research, it was found that limited literature on comprehensive SOC frameworks exists. There are frameworks and literature addressing certain technology aspects of SOCs (Bidou, 2004; Rothke, 2009; Madani, Rezayi, & Gharaee, 2011; RSA, 2011), but a holistic framework covering all the technical aspects, together with the people and processes components, does not seem to exist. According to the Oxford dictionary a framework is *"a set of beliefs, ideas or rules that is used as the basis for making judgements, decisions, etc."* (Oxford University Press, 2011).

A framework thus serves as a reference when planning or building something. It is not a set of instructions that need to be followed to the letter, but is flexible and can be adapted to the situation. The use of frameworks in the design of a product or service offering allows organisations to achieve their objectives with respect to the service or product (Adler, 2007).

There are several IT Frameworks and standards in existence today, and they all address IT Security in some way or the other. Most common of these are Information Technology Infrastructure Library (ITIL), Control Objectives for Information Technology (CoBIT), and ISO/IEC 27001:2005 which is specifically covering information security management (Sahibudin, Sharifi & Ayat, 2008). Architecture frameworks such as The Open Group Architecture Framework (TOGAF) could have been used, but for the purpose of the development of a framework, the SOC is seen as a system, and as such Systems Engineering (SE) principles was decided on, since it provides a mechanism to determine, in detail, the functional requirements of SOCs.

It was decided to use the Telecommunications Management Forum's eTOM process framework. The eTOM framework consists of a hierarchical catalogue of the key business processes that are needed and that are to be followed when running a service-oriented business. SOCs are service-oriented businesses (HP Enterprise Security Business, 2009; Reply Communication Valley, 2011; Nicolett, 2012); supported by people, processes and technology (HP Enterprise Security Business, 2009; Bevis, 2012; McAfee, 2012; RSA, 2013a). The rationale behind the selection of this framework is that it provides comprehensive business processes such as marketing, sales and billing, which are not present in the frameworks and standards used to augment the SOC framework.

Standards and frameworks such as CoBIT, ITIL and the ISO 2000 series compliment and build on each other, and there is a synergy between them. For example, CoBIT focuses on the governance of IT, while ITIL and the ISO 2000 series focus on IT processes (Lew, 2009). However, these frameworks and standards focus on IT service delivery and operational issues and audit requirements, but not on business processes. To this end, the eTOM framework was used to determine business processes, and CoBIT, ITIL and ISO/IEC 27001:2005 will be used to augment the framework. Systems Engineering principles, CoBIT, and ISO/IEC 27001:2005 is discussed further in the following chapter, with reference to their strengths and weaknesses.

2.2 Frameworks and Standards used to define SOCs

SOCs provide situational awareness for organisations on their security posture, reduce risk and downtime, prevent and control threats, ease administrative overhead, serve as an escalation path and assist with audit and compliance (Kelley *et al.,* 2006). In other words, a SOC prevents, detects, reacts and assist in recovering from security related incidents, and in the process assists with compliance.

A SOC receives events from a variety of technology solutions, which could be implemented locally or across a geographically dispersed environment. In this respect, the capability of the technology that interprets the raw data is very important. This is done by the SOC primary technology, namely a Security Incident and Event Monitoring tool (SIEM).

Paradia, (2012) identified process frameworks, standards and methodologies to be used when designing or building operation centers. These are not frameworks for SOCs, but serve to guide the implementation of SOCs as well as their context in information security management.

Table 2-1: Processes, Frameworks and methodologies used in building Operation Centers (Paradia, 2012)

Category / Discipline	Type	Framework / Standard / Methodology
Quality Management and Business Process Management	Frameworks that focus on quality standards applied to specific IT domains (service, security, architecture, general)	TQM, EFQM, ISO 9000, ISO/IEC 2000, TOGAF, ISO/IEC 27001
Quality Improvement	Frameworks that focus on assessment and improvement of processes, performance or other, not focusing on how-to aspects of operating the IT	CMMI, Six SIGMA, eSCM-SP, IT Balanced Scorecard
IT Governance	Frameworks that focus on how to organise the IT function in terms of responsibilities, controls, organisation	AS 8015, ISO/IEC 38500, CoBIT, Management of Risk (M_O_R),
Information Management	Frameworks that focus on how to perform certain aspects of information management, such as procurement, service management, requirements	ITIL, eTOM
Project Management	Frameworks that focus on project, program, and portfolio management, not specifically IT	MSP, PRINCE2, PMBoK, IPMA Complete Baseline

Table 2-1 provides a breakdown of all the process frameworks that could be used when building a SOC.

- From a security domain-specific perspective, ISO/IEC 27001 was chosen. The rationale is that ISO/IEC 27001 covers security in depth. It can be said from an IT security perspective that CoBIT and ITIL is wide, and that ISO/IEC 27001 is deep.
- From an IT Governance perspective, CoBIT was decided on.
- From an operational management perspective, ITIL was chosen. ITIL's focus is on operational aspects such as incident and change management.

- From a business process and management perspective, eTOM was chosen. eTOM encompasses aspects such as sales and marketing as well as product definition, which is lacking from ITIL, CoBIT, and ISO/IEC 27001:2005.

The two prominent frameworks CoBIT (Nicho, 2012; Spafford, Wheeler, & Mingay, 2012; MyBroadband, 2013), and ITIL (Ball, 2006; Roth, 2008; USA, 2011), and the ISO/IEC 27001:2005 standard (ISO / IEC, 2005) are widely used in most organisations, and are mostly used on their own. However, they are not on their own comprehensive enough to serve as an efficient management system. All of these have strengths and limitations, which are discussed further.

2.2.1 Control Objectives for Information Technology (CoBIT)

In terms of IT governance, CoBIT is an internationally accepted framework. It is based on industry standards and best practices, and was developed by the Information Systems Audit and Control Association (ISACA) and the IT Governance Institute (ITGI) to govern the entire IT scope. CoBIT identifies and addresses 7 key IT criteria, confidentiality, integrity, availability, effectiveness, efficiency, reliability and compliance, which auditors can use to audit against. (Lew, 2009).

CoBIT focuses on IT from a business perspective. It is a non-technical framework (ISecT, 2011), and is platform, technology and hardware independent. CoBIT is based on established frameworks such as the Software Engineering Institute's Capability Maturity Model (CMM) (Curtis, Paulk, Chrissis & Weber, 1993), ISO 9000, ITIL and ISO/IEC 27001:2005 as described by Hardy & Heschl (2008). It does not include processes and tasks since it is not a process framework, but a control and management framework. The basic CoBIT principles are shown in Figure 2-1 from System Integrity (2010).

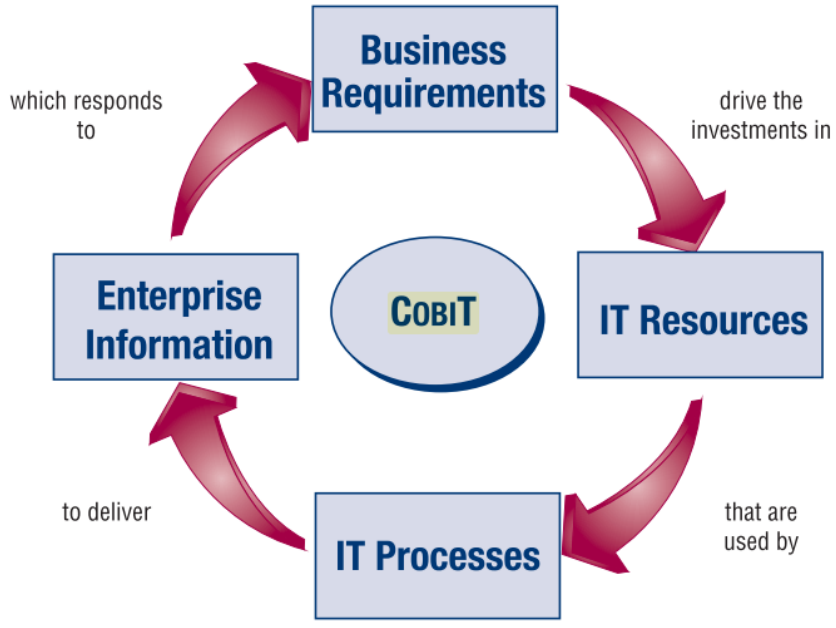

Figure 2-1: Basic CoBIT Principle (System Integrity, 2010)

CoBIT covers 4 domains namely, Plan and Organize, Acquire and Implement, Deliver and Support and Monitor and Evaluate, with thirty-four high-level objectives. This reiterative cycle facilitates the development of clear and applicable policies (Adler, 2007a), and using CoBIT as a supportive toolset, allows managers to understand the gaps between technical issues, business risk and control requirements.

A maturity model is also defined to measure how well IT is managed in the organisation. It evaluates the organisation, which can be rated from a non-existent maturity level (0) to an optimised level (5).

When treating a SOC as a normal business or enterprise, information needs to conform to certain information criteria in order to satisfy business objectives. These are also referred to as business requirements for information. Based on the broader quality, monetary and security requirements, seven distinct information criteria were identified by CoBIT (IBM, 2008; Lew, 2009; Nicho, 2012)

The criteria as identified by CoBIT (IBM, 2008; Lew, 2009; Nicho, 2012) are:

- Effectiveness
- Efficiency
- Confidentiality
- Integrity
- Availability
- Compliance
- Reliability

The CoBIT framework (Hardy *et al.,* 2008) focuses on what an enterprise needs to *do*, and not on *how* it needs to do it. From a security perspective, CoBIT (Guldentops, 2007) provides a process model at a much higher level than ISO/IEC 27001:2005, and will be used to assist in determining a security baseline for the SOC.

The use of CoBIT aspects for the creation of the SOC framework will allow for the mitigation of risk within the SOC itself, the strengthening of security internally, easing of the auditing burden, and reduction of cost while improving consistency of IT and SOC services to customers (Suer, 2012). The rationale for selecting CoBIT 4.1 over CoBIT 5 is that CoBIT 5 was released in June 2012, and its implementation and effectiveness not as rigorously tested as CoBIT 4.1. In addition, CoBIT 4.1 addresses IT processes, and have only two processes (DS4 and DS5) focussing on security and continuity. These aspects better covered in ISO/IEC 27001, so CoBIT is primarily used for processes that are not covered in as much detail in ITIL and ISO. CoBIT 5 was also not yet available during the inception of this study.

2.2.1.1 CoBIT and Security Management

In CoBIT 4.1, guidance on how to define, operate and monitor a system for security is provided in processes DS04 (Manage Continuity) and DS05 (Manage Security Services). CoBIT 4.1 for Information Security addresses the need to describe information security in an enterprise context, as well as the IT functional responsibilities of information security and the aspects that lead to effective governance and management of information security. It also links back information security to enterprise objectives.

In developing the SOC framework, the SOC itself is seen as an enterprise or business entity on its own, and need to be managed as such. CoBIT 4.1 enables information security principles, policies, frameworks, processes, organisational structures, culture, ethics and behaviour, as well as people, skills and competencies (ISACA, 2013). These are all aspects that are applicable to SOCs, and these aspects will be leveraged when developing the framework.

2.2.2 Information Technology Infrastructure Library (ITIL)

The Information Technology Infrastructure Library (ITIL) provides a best practice framework in support of the operational phases of IT service management. ITIL assist with providing a consistent, comprehensive and coherent IT service management framework. It concerns itself solely with IT service management, which in turn focuses on the planning, sourcing, designing, implementing, operating, supporting and improvement of IT services. ITIL specifically supports the effectiveness and efficiency criteria as identified by CoBIT. ISO/IEC 2000 can be used to certify and prove compliance against the ITIL framework. ITIL is currently the globally most widely accepted approach to IT service management (Office of Government Commerce, 2000), and was developed, and distributed by the Office of Government Commerce (OGC) in the United Kingdom (UK). ITIL provides guidance on all aspects of IT service management, and encompasses the following - service strategy, service design, service transition, service operation and continual service improvement as illustrated in Figure 2-2 from NoxGlobe (2011).

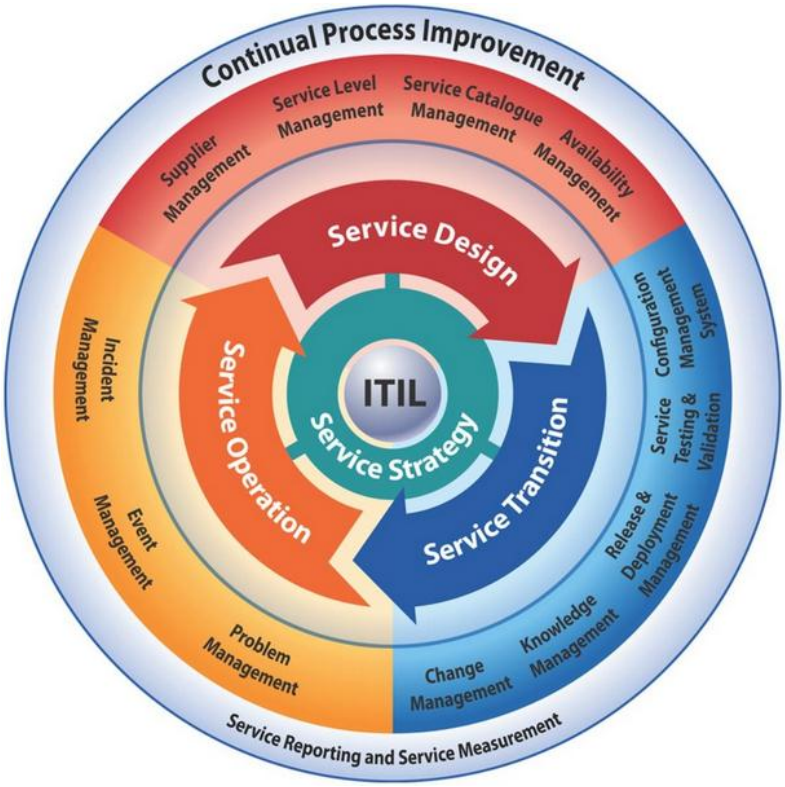

Figure 2-2: ITIL Structure (NoxGlobe, 2011)

The way in which ITIL describes its processes, as well as its implementation approach makes it an attractive option when considering and comparing IT service management frameworks (Sahibudin *et al.,* 2008). It also provides an attractive cost-benefit ratio. ITIL does not define a control framework, but its processes aids in supporting a IT service management control framework. For the purpose of designing and building the SOC framework, the ITIL Service Support and ITIL Service Delivery books will be used. In these books are contained a set of standardised methodologies for for IT operational processes. Processes such as incident management and availability management are included, and seen from a SOC perspective, incident management is a core function. Another SOC core function is a service desk capability. This is also described in the ITIL service delivery book, and includes best practices for managing a central contact point for all clients, internally and externally, consuming SOC services, and needing the ability to register security related calls to the SOC. Aspects such as the monitoring of incidents and communication to customers are also described (Weil, 2010).

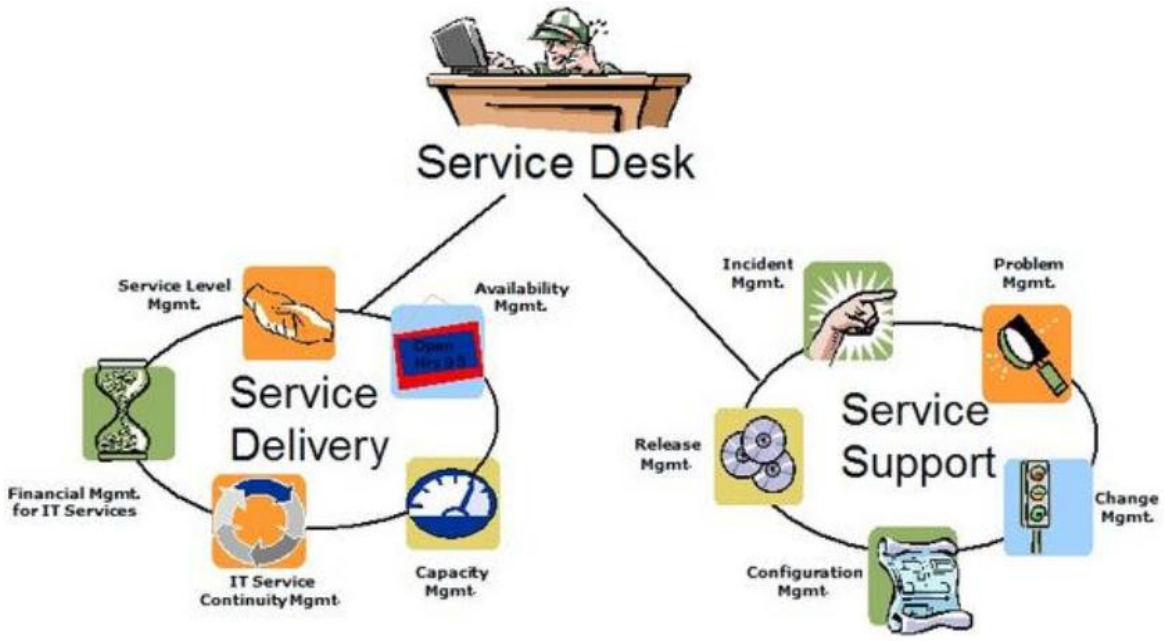

Figure 2-3: ITIL Service Management Processes (Weil, 2010)

Figure 2-3 illustrates the Service Delivery and Service Support components that are integrated into a service desk. SOCs must have a mechanism to capture and communicate incidents to clients, either manually or in an automated fashion.

Over and above the fact that ITIL addresses some of the service aspects of SOCs, it can also contribute to the security of the SOC itself. Furthermore, it can contribute in terms of the security as a service offering to clients. ITIL can improve security in the following ways (Weil, 2010):

- It keeps IT Security business- and service-focused;
- It enables the development and implementation of IT Security in a structured, clear way;
- It ensures that IT Security measures maintain their effectiveness as part of the continuous review requirement;
- It establishes Service Level Agreements (SLAs) described as "a collection of promises. The document records the promises, but not the means or details of execution" (Knowledgetransfer, 2011b) and Operational Level Agreements (OLAs), described as "an internal document, owned by the Service Management Team, that defines the working relationship between different functional areas within an organisation. The OLA sets out the responsibilities for the support and delivery of IT services to Customers." (Knowledgetransfer, 2011a) - which are formalised, documented processes that can be audited; and
- It provides best practices (such as Configuration and Incident Management) that can improve IT Security.

2.2.2.1 ITIL and Security Management

From an ITIL perspective, the management of physical security or personal safety is not covered; neither are the technical details of devising and incorporating security measures. Risk analysis from a security perspective is also not within scope.

Using ITIL, a state of enhanced security can be accomplished by implementing controlled processes. ITIL in itself should not be used to implement security, but the processes as defined in ITIL security management will ensure that the ITIL processes consider security. (Wallhoff, 2005).

2.2.3 ISO/IEC 27001:2005 and ISO/IEC 27002:2005

The historic source for ISO/IEC 27001:2005 was BS 7799, which was published by the British Standards Institute (BSI). Currently, ISO/IEC 27002 actually describes two different documents. These are ISO/IEC 17799, renamed to ISO/IEC 27002:2005 (a code of practice, or a set of security controls), and ISO/IEC 27001:2005 which is a standard specification for an Information Security Management System (ISMS). ISO/IEC 27002:2005 describes the controls in support of ISO/IEC 27001:2005 and mimics the ISO/IEC 27001:2005 sections. It outlines controls and control mechanisms which may or may not be applicable to an organisation. It covers twelve (12) sections. They cover 39 key elements with 133 controls. In order to determine applicable controls, security requirements should first be established. The twelve ISO/IEC 27002:2005 sections are depicted in Figure 2-4 from GetITRight (2013).

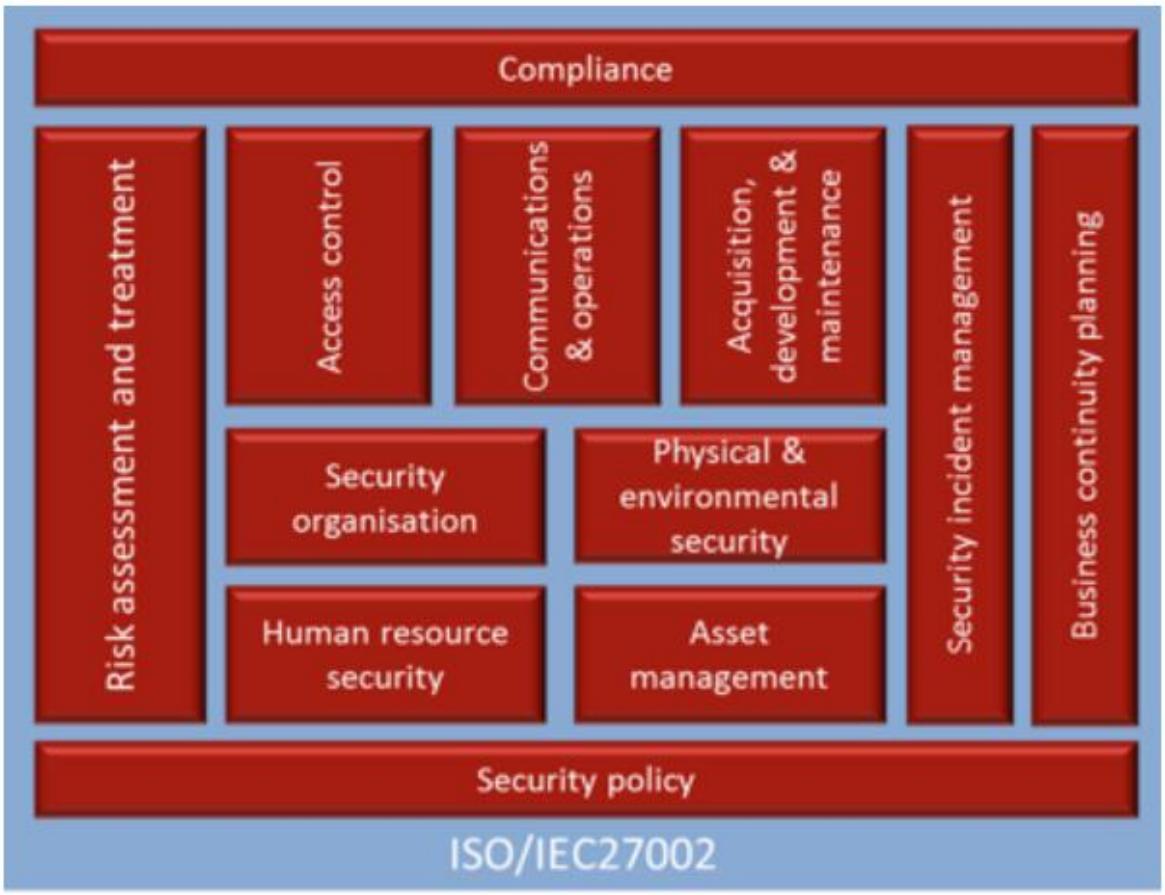

Figure 2-4: ISO 27001 Sections (GetITRight, 2013)

ISO/IEC 27002:2005 follows a risk-based approach, and the importance of a risk management strategy and methodology is accentuated throughout the standard. Organisations should further identify only those controls applicable and relevant to them by using a risk management approach. It is therefore not necessary to implement all controls specified in ISO/IEC 27002:2005. Legal requirements and generally accepted best practices were used in determining the ISO/IEC 27002:2005 guiding principles. ISO/IEC 27002:2005 relies on legal and statutory requirements as drivers, and leverage off best practices. Critical success factors are defined and communicated to stakeholders. These principles are listed in Table 2-2.

Table 2-2: ISO 27002 Guiding principles (Hardy *et al.,* 2008)

Legal Requirements	Best Practices	Critical Success Factors	Communication to third parties
Protection and non-disclosure of personal data	Information security policy	The security policy, its objectives and activities should reflect the business objectives	Users should be trained in an adequate manner
Protection of internal information	Assignment of responsibility for information security	The implementation should consider cultural aspects of the organisation	A comprehensive and balanced system for performance measurement, which supports continuous improvement by giving feedback, should be available
Protection of intellectual property rights	Problem escalation	Open support from and engagement of senior management should be required	
	Business continuity management	Thorough knowledge of security requirements, risk assessment and risk management should be required	
		Effective marketing of security should target all personnel including members of management	

2.2.3.1 ISO/IEC 27001:2005 and Security Management

ISO/IEC 27001:2005 defines 11 categories with 133 security control strategies providing assistance and guidance to security specialists in the implementation of information security within an organisation. The ISO/IEC 27001:2005 controls are also referred to as security measures or defensive measures (Warren, 2010). ISO/IEC 27001:2005 also provides a shared model, which can be followed to implement and operate an Information Security Management System (ISMS). Willet (2008) describes an ISMS as "*a management system from a business risk perspective, that has the purpose to establish, implement, operate, monitor and maintain an a secure posture for an organisation".*

The establishment of security requirements as stated by ISO/IEC 27001:2005 can be achieved by using three main sources (ISO/IEC 27001:2005, 2005):

- By following a risk-based approach, and conducting a risk assessment. While performing the risk assessment, organisational strategy and objectives have to be kept in mind. The risk assessment result will assist and guide management as to the prioritisation of risks and actions that need to be taken to manage information security risk.
- Requirements such as legal, statutory, and regulations specific to country and industry, as well as contractual requirements that the organisation need to fulfil. These requirements could also be applicable to an organisations partners, suppliers, service providers and contractors. The social and cultural environment of the organisation also needs to be taken into consideration.

- Principles, objectives and business requirements that an organisation has developed to govern information and data processing in support of business processes.

Once the security requirements of a SOC have been determined, appropriate controls must be selected and implemented.

ISO/IEC 27001:2005 consists of eleven clauses, and each clause contains security categories. The areas as listed by ISO/IEC 27001:2005, (2005) are:

- Security Policy
- Organizing Information Security
- Asset Management
- Human Resources Security
- Physical and Environmental Security
- Communications and Operations Management
- Access Control
- Information Systems Acquisition, Development and Maintenance
- Information Security Incident Management
- Business Continuity Management
- Compliance.

The 11 ISO/IEC 27001:2005 categories contain control objectives which state goals and achievements, and list the controls, which could be applied to achieve the stated goals and objectives (i.e. the *how*). From a SOC perspective, these will address some aspects of the SOC structure, such as policies, procedures and responsibilities. This addresses some of the requirements as expressed in the SOC functional, service, business and people requirements. ISO/IEC 27001:2005 will assist in securing the SOC, and this approach allows SOC management to monitor and control security, while minimizing security risk. Aspects related to SOC service delivery, SOC Operations and SOC management will be determined from the ISO 27001:2005 standard. Whereas CoBIT addresses IT processes, ITIL covers operational aspects and processes, and ISO/IEC 27001:2005 security, none of these address business processes such as sales, marketing and other aspects specifically related to the "business of doing business", The Telecommunications Management Forum's eTOM framework provides a mechanism to identify, and address these business aspects not covered by the others.

2.2.4 Telecommunications Management Forum

The Telecommunications Management Forum is the largest global trade association with over 900 member companies (TMForum, 2013). The focus of the Telecommunications Management Forum, is to harness digital ecosystems in the Telecommunications domain. This includes Telecommunication service providers, business and digital and infrastructure service providers. The TM Forum Framework is a suite of best practices and standards that is globally accepted by over 900 companies (TMForum, 2013). It is constantly reviewed, accepted by industry, and tested and validated by businesses across the globe. It consists of a Business Process Framework, Information Framework, Application Framework and an Integration Framework.

The Telecommunications Management Forum frameworks (Jiejin, 2009) are known as the New Generation Operation Systems and Software (NGOSS). The purpose of the NGOSS frameworks are to assist users to analyse their business processes against industry processes in the Telecommunications domain, as well as industry accepted standards and applications.

The gap between data communications and telecommunications serves as the driver for the TM Forum's New Generation Operations Systems and Software (NGOSS) initiative. NGOSS aim is to enable flexible and timeous integration between Business Support Systems (BSS) and Operations Support Systems (OSS) in the Telecommunications environment.

Four NGOSS frameworks are described by the Telecommunications Management Forum (Jiejin, 2009). These are illustrated in Figure 2-5 as taken from TMForum, (2013)

- Business Process Framework (eTOM)
- Information Framework (SID)
- Integration Framework (TNA)
- Application Framework (TAM)

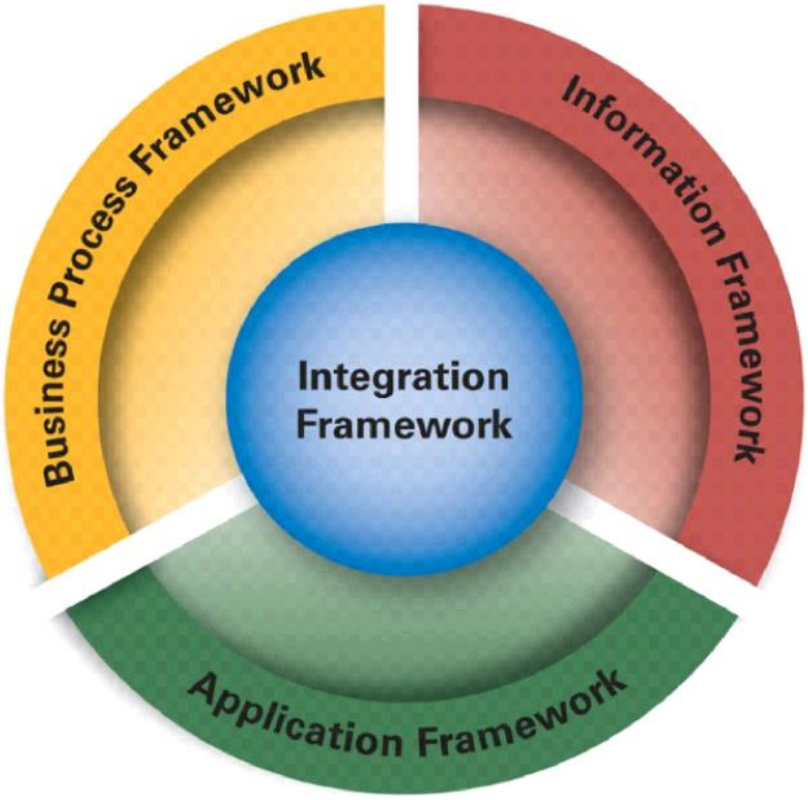

Figure 2-5: TM Forum NGOSS Frameworks (TMForum, 2013)

We have identified the TM Forum framework as ideal for building the SOC framework, for the following reasons as discussed by Jiejin, (2009), and adapted by the author for SOCs:

- Business activities across all levels of the SOC as a singular business entity, and the SOC as part of a business entity are categorised.
- For SOC managers, the eTOM framework assist in the development of a SOC business structure, the assessment of the process structure against the framework, as well as the identification of process components, their interactivity with existing business processes and business roles they rely on.
- The eTOM business process model is widely adopted in the industry (TMForum, 2013).
- It can serve as a blueprint for standardised business activities, which can provide SOC designers with a starting point and assist with future development.
- It identifies marketing processes which is done by neither CoBIT, ITIL or ISO/IEC 27001:2005.

- It identifies Enterprise Management processes, supported by ITIL. These processes will be augmented by CoBIT and ISO/IEC 27001:2005.
- It focuses on Fulfilment, Assurance and Billing & Revenue Management.

The TM Forum framework is a comprehensive framework addressing business issues such as marketing and sales, as well as strategy, infrastructure and product, operations and enterprise management.

The TM Forum Telecom Operations Map (TOM) was used as the underlying basis or principle for the development f the enhanced Telecom Operations Map (eTOM). The enhanced Telecom Operations Map provides a collection of business processes that are required by service providers. It also determines and defines key business elements and how the work together. The framework also covers aspects such as procurement processes, development and implementation of a service provider environment.

One of this model's advantages is that it establishes a common vocabulary for both business and functional processes. It can also describe a framework to assist in the development of business practices focussing on customers. The eTOM Framework is also be useful in guiding the business organisation of a SOC, as well as identifying and defining interfaces between business processes internally, and business and the customer (Milham, 2004).

At the lowest level, eTOM is a model or framework for Telecommunication companies to implement enterprise practices. It is broken down into three levels (Cisco Systems, 2009):

- Strategic, Infrastructure and Product, including marketing and offer management, service and management resource development as well as supply chain development and management. These are all aspects that are not addressed by other frameworks and architectures such as ISO/IEC 27001:2005, ITIL and CoBIT.
- Operations, which includes Customer Relationship management, service management and operations, resource management and operations and supplier/partner relationships.
- Enterprise management, which includes strategic and enterprise management, risk management, enterprise effectiveness management, knowledge and research management as well as financial and asset management.

The benefits of using the eTOM framework are defined by Cisco Systems, (2009) as follows:

- A standard framework consisting of a common terminology and a classification scheme to describe business processes and their fundamental building blocks is made available for use when designing SOCs.
- The framework can be used as an authority for implementing enterprise-wide methods to the development of business processes.
- It assists with the understanding and management of IT portfolios in terms of business process requirements by providing a common basis or framework.
- Cost and performance indicators can be improved on, and existing artefacts can be re-used by using the framework to develop consistent, end-to-end process flows.
- Using the framework improves the chances of commercial off the shelf (COTS) applications being integrated at a lower cost than custom-built applications (TMForum, 2013).
- It can serve as a layout for process direction, and provides an unbiased reference point from which to assist with internal process re-engineering, as well as with general working agreements with other providers.

In summary: ITIL will be used from an operational perspective, ISO/IEC 27001:2005 from a security perspective, CoBIT from a governance perspective and eTOM from a business process

perspective. eTOM encompasses all business-related aspects that are not covered by ITIL, CoBIT or ISO/IEC 27001:2005, such as sales, marketing and business development.

In order to be able to identify the elements of eTOM, CoBIT, ITIL and ISO/IEC 27001:2005 that are to be used, we need to identify the functional requirements of SOCs.

In the determination of the functional requirements of SOCs, systems engineering principles will be used. These functional requirements will then be mapped back to CoBIT, ISO/IEC 27001:2005 eTOM and ITIL.

2.3 Principles used in defining SOC framework

System Engineering processes and principles will be followed to determine the functional specifications of a SOC. Systems engineering will therefore be discussed here.

2.3.1 Systems Engineering

The International Council of Systems Engineers (INCOSE), in the INCOSE Systems Engineering Handbook v3.2 (INCOSE, 2010), defines systems engineering as follows: *"Systems engineering is an interdisciplinary approach and means to enable the realization of successful systems. It focuses on defining customer needs and required functionality early in the development cycle, documenting requirements, and then proceeding with design synthesis and system validation while considering the complete problem: operations, cost and schedule, performance, training and support, test, manufacturing, and disposal. SE considers both the business and the technical needs of all customers with the goal of providing a quality product that meets the user needs."*

According to the INCOSE handbook, a system is defined as *"an integrated set of elements that accomplish a defined objective"* (INCOSE, 2010). Elements included are hardware, software and firmware products, people, processes, information, routines, as well as elements supporting the systems to be designed.

From this definition it can be seen that a Security Operation Center can be classified as a system, and should be designed as such.

ISO/IEC 15288:2008 (ISO/IEC 15288:2008, 2008) (which served as input for the INCOSE handbook (INCOSE, 2010) identifies seven (7) System Lifecycle stages. These are Exploratory Research, Concept, Development, Production, Utilisation, Support, and Retirement.

For the purpose of determining the functional requirements of a SOC we will focus on the Development stage, since this stage encompasses the Systems Requirements Analysis, the creation of Functional Requirements and the determination of the MOE's).

An advanced or 'next-generation' Security Operations Center can be classified as a 'System of Systems'. According to Krygiel, (1999) "Systems-of-Systems" (SoS) are systems of interest whose system elements are systems themselves. These typically entail large-scale interdisciplinary problems involving multiple heterogeneous, distributed systems. These interoperating collections of component systems usually produce results that are unachievable by the individual systems alone."

These next-generation SOCs would be combining different systems such as SIEM, Electronic Governance, Risk and Compliance (GRC), Change Management and Vulnerability Management.

Table 2-3 lists the seven generic system life-cycle stages together with their purpose and decision gates as reproduced from INCOSE, (2010).

Table 2-3: System Engineering Lifecycle stages (INCOSE, 2010)

LIFE-CYCLE STAGES	PURPOSE	DECISION GATES
EXPLORATORY RESEARCH	Identify stakeholders' needs Explore ideas and technologies	Decision Options • Proceed with next stage • Proceed and respond to action items • Continue this stage • Return to preceding stage • Put a hold on project activity • Terminate project
CONCEPT	Refine stakeholders' needs Explore feasible concepts Propose viable solutions	
DEVELOPMENT	Refine system requirements Create solution description Build system Verify and validate system	
PRODUCTION	Produce systems Inspect and verify	
UTILIZATION	Operate system to satisfy users' needs	
SUPPORT	Provide sustained system capability	
RETIREMENT	Store, archive or dispose of the system	

The next-generation SOC's capabilities will be heavily supported by the SOC primary technology component, which is the SIEM. A multi-national effort is underway to achieve advancements in the areas of SIEMs. This is called project MASSIF, and stands for "MAnagement of Security information and events in Service InFrastructures" (ATOS Research, 2010). Their main purpose is the development of a next-generation SIEM framework, specifically developed for the service infrastructure. The following are key objectives, - to support intelligent, scalable and multi-level and multi-domain security event processing, as well as predictive security monitoring. As per the MASSIF FP7 Project (ATOS Research, 2010), future SIEM technologies will offer and integrate the following systems:

- Scalable, dependable and multi-level event collection;
- Multi-level event correlation;
- Predictive security analysis;
- Multi-level security event modelling; and
- Process and attack simulation.

The purpose of System Requirements according to ISO/IEC 15288:2008 (ISO/IEC 15288:2008, 2008) is "*to transform the stakeholder Requirement driven view of desired services into a technical view of a required product that could deliver those services. This process builds a representation of a future system that will meet stakeholder requirements and that, as far as constraints permit, does not imply any specific implementation. It results in measurable system requirements that specify, from the supplier's perspective, what characteristics it is to possess and with what magnitude in order to satisfy stakeholder requirements.*"

System requirements form the basis of system definition, and will form the basis of the design, integration and verification of the system. As part of the System Requirement Analysis, Measures of Effectiveness (MoE's) will also be generated. The INCOSE Systems Engineering Handbook v3.2 defines MoE's as the *"operational measures of success that are closely related to the achievement of the mission or operational objective being evaluated, in the intended operational environment under a specified set of conditions"* (INCOSE, 2010). MoE's are specific properties that a technical solution must exhibit to be acceptable to the acquirer (Roedler & Jones, 2005). This distinction is important when trying to measure the performance of SOCs and when developing a classification system.

Figure 2-6 as reproduced from INCOSE, (2010), supplies the context for the Requirements Analysis Process (INCOSE, 2010), and lists inputs, controls and enablers supporting activities

to provide the output – in this instance, the system requirements. In order to be able to determine the requirements of the system, which in this case is the SOC system, all systems and elements applicable to a SOC needs to be identified. Technical processes as defined in ISO/IEC 15288:2008 (ISO/IEC 15288:2008, 2008) are used to:

> *"define the requirements for a system, to transform the requirements into an effective product, to permit consistent reproduction of the product where necessary, to use the product to provide the required services, to sustain the provision of those services and to dispose of the product when it is retired from service".*

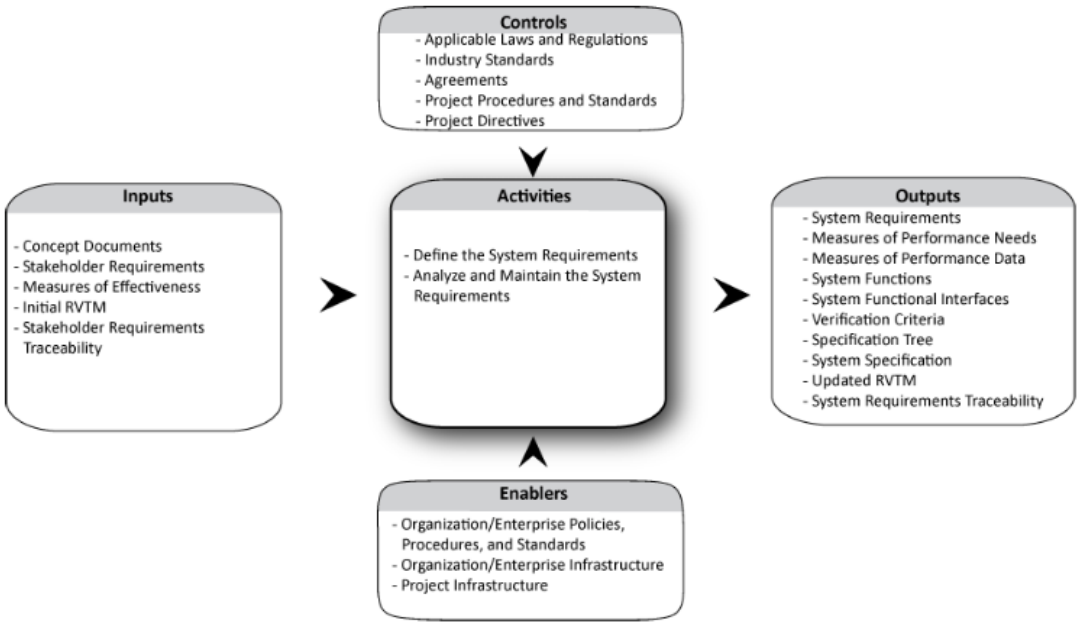

Figure 2-6: System Engineering Requirements Analysis Process (INCOSE, 2010)

These processes are technical, project, agreement, organisational, project enabling, and tailoring. System Requirements Analysis forms part of the technical process. In order to determine the SOC system requirements from which the SOC functional and other requirements will be determined, a System Requirements Analysis will be performed. Different sources can serve as input to system requirements, such as the external environment, organisational environment and project environment. All of these sources have to be kept in mind when doing the Requirements Analysis. The different sources and their context are shown in Figure 2-7 as reproduced from INCOSE, (2010):

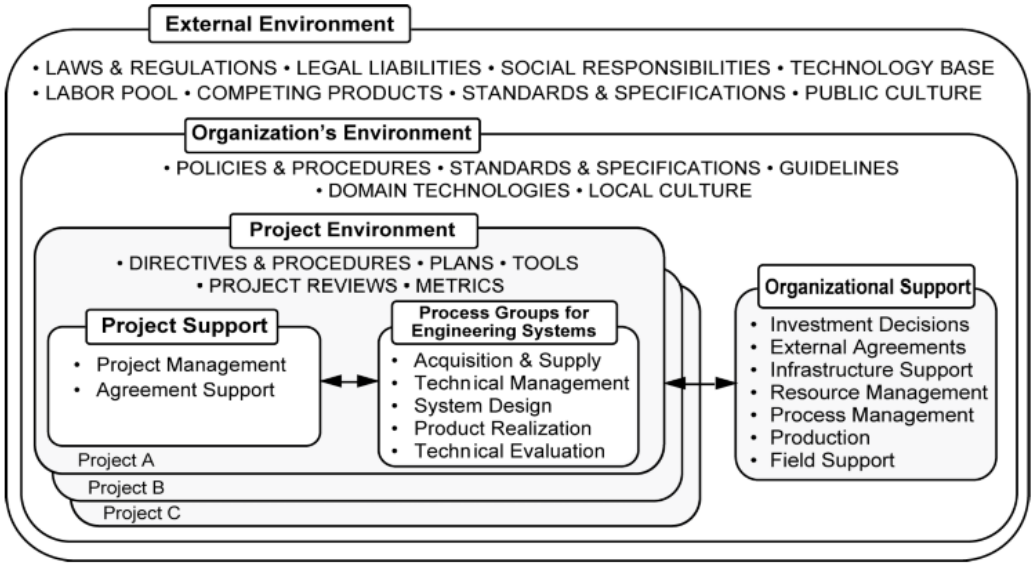

Figure 2-7: Requirements Analysis Sources and Context (INCOSE, 2010)

In determining the SOC system requirements, the external environment as well as the organisational environment (with all its applicable elements) will be used.

2.4 Summary

In chapter two ISO/IEC 27001:2005, ITIL, CoBIT and eTOM were reviewed. Their inclusion in and fit with the SOC framework was discussed, and the rationale was supplied. Figure 2-8 as reproduced from Lew (2009) shows the integration of frameworks and standards within an organisation, as well as the business functions where CoBIT, ITIL and ISO 27001 are applied.

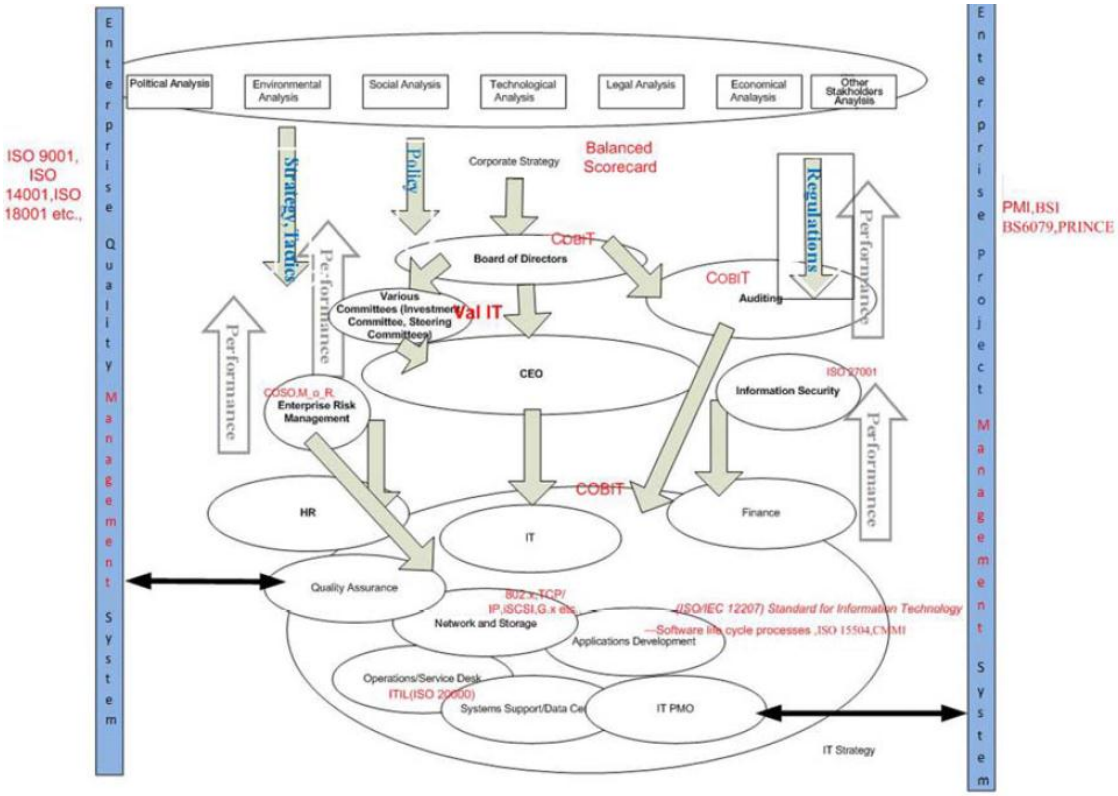

Figure 2-8: Frameworks and Standards in a Business Context (Lew, 2009)

As illustrated in Figure 2-8, some frameworks exist to address the different business processes. However, no framework exists that focuses on the entire business.

The IT environment should be managed as part of a routine. To assist with this task, effective management policies and procedures should be developed. To further enable the routine management of the IT environment, standards and frameworks should be adopted to assist with the implementation of good SOC processes. This approach also avoids delays and reiterative process designs. The frameworks and standards adopted and used in the development of the SOC framework have to be consistent and repeatable.

The focus of CoBIT is on the business processes and on its auditability. ITIL's focus is on IT Service Management, while ISO/IEC 27001:2005 and 27002:2005 focuses on IT security. It can be said that CoBIT and ITIL are wide, while ISO/IEC 27001:2005 is deep with regards to IT Security. Neither CoBIT or ITIL, nor ISO/IEC 27001 or 27002, address business aspects such as sales and marketing.

CoBIT defines *'what'* should be done in terms of IT management tasks, ISO/IEC 27001:2005 defines the *'what'* and the *'how'* in terms of securing the SOC, and ITIL provides the *'how'* for

service management aspects. In order to achieve that effect, we will tailor the above frameworks and standards to support governance, to define requirements, to facilitate continuous improvement by assessing maturity, and to be used as a framework for auditing and assessing the SOC.

CoBIT and ISO/IEC 27001:2005 are complementary. They both identify best practices, with ITIL focusing on service management and ISO/IEC 27001:2005 focusing on information security best practices. Both use the Plan-Do-Check-Act (PDCA) model as described by Sheikhpour and Modiri (2012). From an ITIL perspective, most of the security controls that are defined form part of service management.

Keeping these facts in mind, ITIL will specifically be used for service management, ISO/IEC 27001:2005 for information security management and CoBIT for process management.

Figure 2-9 depicts the areas in which the different frameworks and standards are applicable.

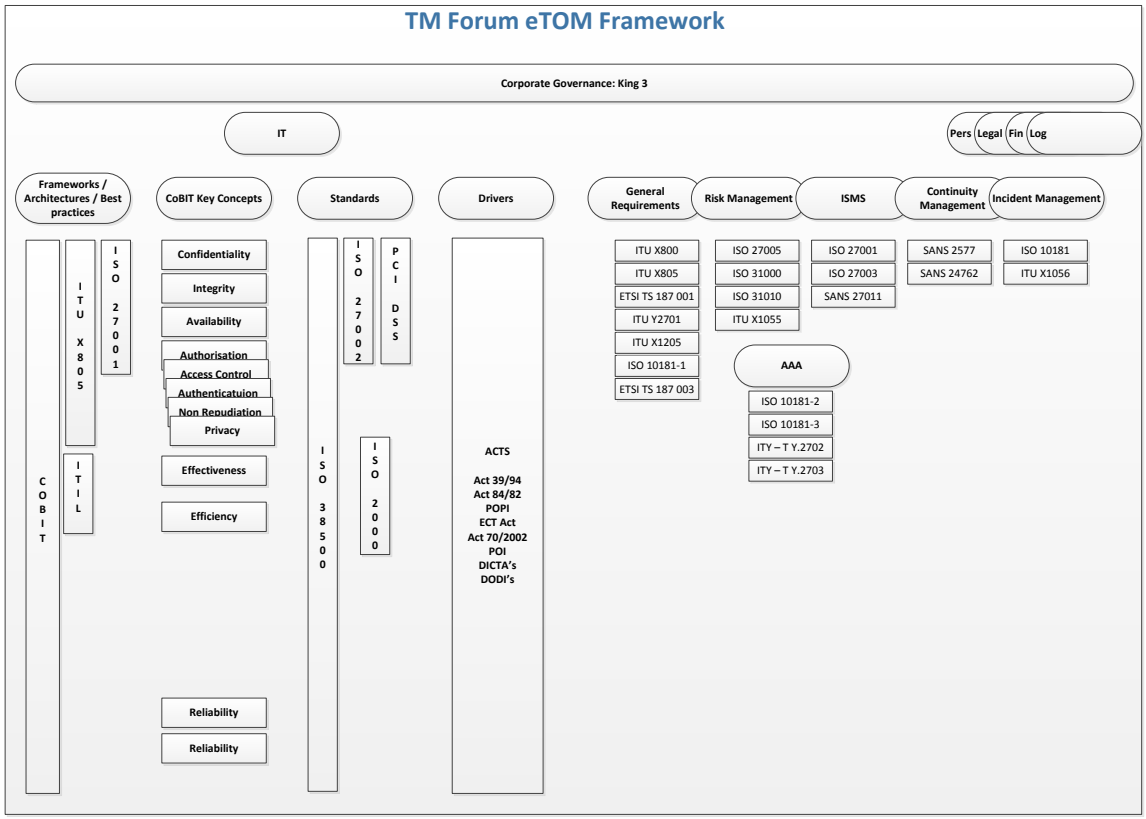

Figure 2-9: Perspective of Standards and Frameworks to Key Concepts

Figure 2-9 shows that CoBIT addresses all aspects from an IT management perspective, ITIL's focus is towards IT Operations and ISO 27001 addresses IT Security in detail. The eTOM framework addresses all aspects of a business, and does not only focus on the IT business silo. The eTOM business process framework will be used as the basis for the SOC framework, and augment gaps or suggest improvements based on CoBIT, ISO/IEC 27001:20005 and ITIL.

System Engineering principles will be used to determine SOC functional requirements, and Measures of Effectiveness (MOE's) will be determined and applied to the SOC functional requirements.

Chapter three will focus on the process used to determine SOC functional requirements, on the SOC functional requirements itself and on the measures of effectiveness.

3 SOC Functional Requirements Analysis

3.1 Introduction

In chapter two, existing frameworks and standards applicable to SOCs were identified. These were chosen for their completeness, their applicability to SOCs as well as for acceptance by industry.

In this chapter we will utilise System Engineering principles to determine SOC functional requirements, in other words, what does a SOC do? This is the most important part of the study, since these functional requirements have to be complete, future-proof and applicable to SOCs as an independent business (MSSPs) as well as to in-house SOCs.

These functional requirements will be mapped back to the identified frameworks and standards to develop a SOC framework. SOC requirements are grouped into three categories:

- SOC functional requirements;
- SOC service requirements; and
- People requirements.

Once this has been addressed, Measures of Effectiveness (MoE's) for each function will be determined.

3.2 Functional Requirements Approach

In following a holistic approach to security (HP Enterprise Security Business, 2009) we need to focus on people, processes and technology. Determining the technology functional requirements is beyond of the scope of this work, since the focus is on SOC functional requirements instead of on technical requirements. SOC technical requirements will be addressed in future work.

However, all information is exposed to these three elements. Technology is used to store, transmit, query and process information. Processes are applied to manipulate the information as part of a service that the organisation provides, or as part of business operations. People access the information, and have to manipulate it according to business processes (Von Solms & Posthumus, 2004).

Bandor (2007) states that policies and standards govern or constrain operations, processes describe what must happen to build products, and procedures describe or give step-by-step instructions on how to implement the process.

In answering the research questions as well as in developing the framework, we will divide SOCs into people and processes, and address each of these elements individually. After this has been done, policies, standards, processes and procedures applicable to people and technology, as well as applicable SOC processes and procedures, will be identified and mapped back to the identified standards and frameworks. The requirements are determined as stated below by using System Engineering principles. The tasks to be completed for each component are as follows:

SOC Functions and Processes

- Determine SOC functional requirements;
- Determine SOC service functions; and

- Determine SOC business requirements, inclusive of people aspects as per the requirements listed in Figure 3-1:

People

- Determine aspects related to the "human" element when building SOCs. These include staffing, career paths, facilities, access control, etc. Industry standards and best practices will be used; and
- Map functional, business (inclusive of people aspects) and service functions to industry accepted frameworks and standards (CoBIT, ISO/IEC 27001:2005 and ITIL) policy, process and procedure requirements.

The framework development approach is depicted in Figure 3-1. It should be noted that the SIEM technology portion is out of the scope of this thesis insofar as no functional or technical requirements and MoE's for SIEM will be determined. These would be addressed as part of future studies. The framework itself will focus on people and process aspects of SOCs.

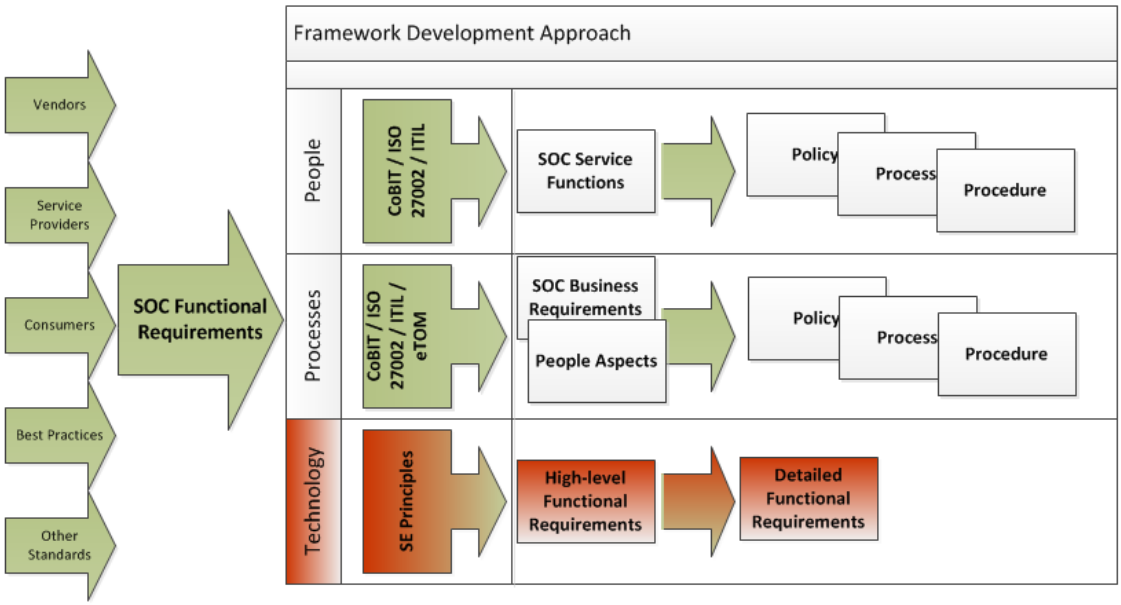

Figure 3-1: Framework Development Approach

The approach followed would be to determine the SOC requirements by using various sources such as vendors, standards and service providers. This will provide the SOC requirements, which will in turn be broken down into three components namely business requirements, service requirements and people aspects.

Defining the capabilities of a SOC can be a daunting task, since most vendors and literature refer to the technical capabilities of SIEM technology, and not to the SOC capabilities per se. To this effect, one has to carefully consider all literature, and identify only those capabilities that are applicable to the intrinsic services of the SOC. The SOC functional capabilities will be derived in this section by an analysis of what all of the major vendors, and standards indicate as being primary aspects or functionalities of a SOC.

Hewlett Packard (HP) groups SOC capabilities into five generations (Hewlett-Packard, 2013):

- First-generation SOC - were ad hoc, understaffed and utilised emerging technologies. Their responsibility was mainly to monitor and manage security technical controls.
- Second-generation SOC - is categorised as a period of malware outbreaks. This era saw the beginning of vulnerability tracking and formalised system patching. During this period security monitoring and management services were commercialised, constituting the advent of Managed Security Service Providers (MSSPs). The big focus

during this period was on intrusion detection systems. The concept of security information event monitoring (SIEM) was introduced towards the end of this period.

- Third-generation SOC - was marked by the organisation and expansion of cybercrime. Malware changed from worms to targeted attacks. Crisis and incident management were formalised by Computer Incident Response Teams (CIRTs).
- Fourth-generation SOC - could be recognised by the publicity of a politically motivated threat landscape, which initiated the advent of hactivism. Organisations began to realise that intrusions will happen, regardless of the technical and other preventative technologies that are in place. The focus during this era has shifted from detection and prevention to exfiltration, detection and containment.
- The 5th Generation (5G) - is still evolving. Most security products provide end-point solutions using signatures to detect malware. However, the threat comes from human adversaries. The 5G SOC recognises the changes in the threat landscape, and approaches the challenge holistically by providing counter-intelligence, surveillance, criminal psychology and analytical thinking training to augment the deployed technology. These SOCs also realise that security programs need to be active, engaged and intelligent.

Various service providers formed part of the research, and a collection of the SOC functional aspects and requirements were determined from their marketing collateral, service catalogues and function lists. There was also a differentiation made between MSSPs and in-house SOCs. MSSPs sell their SOCs as a service with the rationale being that they can leverage off economies of scale to lessen the financial burden on SOC service consumers. In-house SOCs are funded entirely by the organisation. A comparison is provided in Table 3-1. The functions and capabilities are listed per vendor in the following section.

Table 3-1: SOC Service providers' comparison

	HP	RSA	Symantec	IBM	McAfee	Dell	SecureOps	HCL	T-Systems	ACS	CSS
Counter Intelligence	X										
Surveilance	X										
Integrated Threat Intelligence		X	X	X	X					X	
Incident Response		X		X	X	X	X				
Asset Criticality rating		X									
Aggregation and Analysis of intelligence data		X							X		
Correlation of content intelligence data		X	X	X				X	X		
Analytic intelligence capabilities		X	X								
Workflow automation		X									
24x7 Monitoring			X	X	X	X	X	X	X		
Forensic Analysis					X						
In-house research						X					
Reporting											X
Vulnerability Management										X	

The capability of the 5G SOC, as mentioned by HP, is important from the perspective of creating a framework that includes all these capabilities in order to ensure a SOC framework that caters for the currently understood state of security risks.

RSA, the security division of EMC, recently developed a next-generation SOC offering (RSA, 2013b). In their literature they state that their offering is able to assist clients to institute the core infrastructure of security operations. Their service includes the integration of threat intelligence and incident response as part of the security operations, and also the ability to capture asset criticality to assist with prioritisation and categorisation. They also boast a repeatable and continuous service delivery framework. The key operational areas that are defined by RSA (RSA, 2013b) are:

- Aggregation and analysis of threat intelligence data;
- Correlation of content intelligence data throughout the organisation;
- Deployment of solutions that provide advanced analytic intelligence capabilities; and
- Development of security operations processes and procedures and the automation of related workflows.

Symantec launched a new Global Security Operation Center in the United States. They have an international presence with staff deployed globally. They strive to provide visibility of security related activity across the organisation's infrastructure. They also have their own threat intelligence capability, which Symantec offers as a service to clients. They further provide advanced correlation and analysis capabilities (Symantec, 2012).

IBM lists the capabilities of their Virtual SOC as 24x7x365 event monitoring, event handling and analysis, threat intelligence and threat summaries, event correlation and analysis, as well as analysis of past and current events (IBM, 2104).

The capabilities listed by McAfee, (2010) are 24x7 monitoring, security event recognition and response, event and incident resolution, situational awareness, forensic analysis and threat intelligence. As part of their SOCs' capabilities, Dell SecureWorks (Dell, 2013) lists 24x7x365 service delivery, self-sufficient certified analysts, remediation support, detection of and response to incidents as well as their own in-house research capability. Monitoring on a 24x7 basis as well as automated or self-service incident management are some of the capabilities offered by SecureOps (SecureOps, 2013).

HCL (2014) mentions 24x7 monitoring and management (including event correlation), flexible service delivery models that are leveraging off their processes and procedures, guaranteed service delivery using ITIL best practices and an ISO/IEC 27001:2005- as well as an ISO/IEC 9001-certified SOC as their capabilities. T-Systems (2013) lists capabilities as 24x7 monitoring, log analysis using correlation rules and alerting on anomalies.

South African based Altech Card Solutions (Altech ACS, 2013) lists their capabilities as access to experienced analysts, proven processes, threat intelligence, detection and response to threats as well as vulnerabilities. The capabilities of Chameleon Security Services (Chamelion Security Services, 2013), also a South African-based company, are automated log file interrogation and reporting, alerting on critical events, storage of categorised and classified log files, and the monitoring and tracking of remediation processes against SLA.

A Security Operation Center's (SOC) primary goal is to monitor the security of infrastructure, and to provide the capability to detect, analyse, respond to and report on security-related incidents (Arcsight, 2009; Kelley *et al.,* 2006; Milne, 2005; MindPoint Group LLC, 2011; Rothke, 2009). A comparison between services offered by different vendors is included in Appendix G. SOCs must also provide security metrics to assist organisations in assessing and funding security initiatives. Jansen, (2009) discusses how security metrics allow for tactical oversight, enabling the ability to monitor and report on the security posture of an organisation's systems in real time, to gauge the effectiveness of technical controls and to provide reporting and trending data.

The Statement on Auditing Standards (SAS) defines a SOC as "a subset organization within the Network Operations Center (NOC) that provides front-line defence against cyber threats and is the nucleus of all information and Internet security operations. The SOC provides

continuous protection, detection and response capabilities against threats, remotely exploitable vulnerabilities and real-time incidents on the networks." (Protz, 2005).

SOCs should also be able to integrate different security technical controls, as well as correlate between them (HP Enterprise Security Business, 2009; Milne, 2005; Yuan & Zou, 2011) and ensure their continual effectiveness (Dempsey; Johnson; Scholl & Stine, 2011). Furthermore, SOCs should provide information on latest threats and vulnerabilities as well as information on security countermeasures (Dempsey *et al.,* 2011; Kelley *et al.*, 2006). In other words, a SOC should be able to assist with and co-ordinate mitigation and remediation efforts.

SOC functions also include aspects such as vulnerability management, configuration changes on security controls using a change management process, protection of intellectual property and also asset tracking, and the recovery of assets. (Cisco Systems, 2007). Depending on the mandate of the SOC, there should also be a capability to manage network and security devices (Reply Communication Valley, 2011). Finally, SOCs should be able to provide forensic and investigation capability (Pinkard & Curry, 2006). This implies that events should be stored in a forensically secured database (Afzaal, 2012). Since the advent of Advanced Persistent Threats (APTs), SOCs also need to change or evolve their analysis process as well as their incident response process. They would need knowledge of the threat, which implies an analytical capability (Hutchins, 2010). APT's are attacks with the aim to achieve financial or military gain.

The most basic model of a SOC involves that data from multiple sources are fed into a repository and used by human analysts for the purpose of operations, including interpretation, correlation, storing and archiving (Amoroso, 2010). Having access to all this information, a SOC should also provide strategic advice and guidance (RSA, 2013a), as well as various reports and visualisations (Fischbach, 2008; Yuan *et al.,* 2011). Some of the functionality could be added at a later stage, but there are the critical, required functions that every SOC must offer as a minimum. These can be seen from the SOC's primary goals, and include:

- Event Log Collection and Management;
- Real-time Monitoring, and analysis ability;
- Incident Management;
- Reporting and visualisation;
- Providing Strategic advice and guidance and Threat Intelligence;
- Forensic and Investigative functionality;
- Vulnerability Management;
- Business Impact Assessment.

Other functions which could be offered, but that are not critical or required, are:

- Change Management;
- Network and Security Device Management; and
- Security Awareness Training

There was an inconclusive view on the requirement for security awareness training, change management and network and security device management. These functions were thus excluded as primary functions. The framework itself is modular, and these aspects can be added or omitted as requirements change. The primary SOC functions are event log collection and management, monitoring and analysis, incident management, reporting and visualisation, strategic advice and guidance, identification and reaction to threats, monitoring and correlation and workflow. Secondary functions as identified are security awareness training, a forensic and investigative function, device management function, change management function and vulnerability management function.

Figure 3-2 shows the functions with their responsible components, i.e. people, process or technology as well as their dependencies indicated by the arrows:

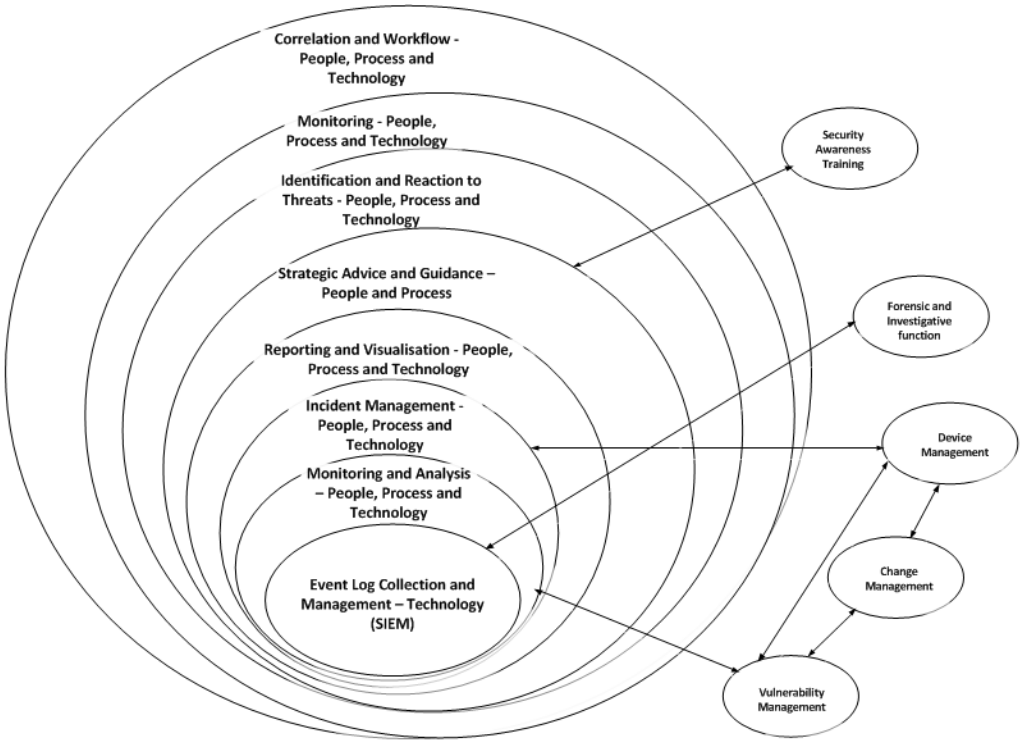

Figure 3-2: SOC Functional Requirements

Now that the SOC functional requirements have been established, the service requirements need to be determined. Whereas the functional requirements determines the operations and activities that systems must perform, service requirements focus on the infrastructure itself, and how it is managed and operated.

3.3 SOC Service Functions: Processes and Procedures

SOCs also include a service aspect that needs to be addressed. Three components are identified when building SOC services. These are people, processes and technology. SOCs should have clearly defined processes that evaluate, control, improve, predict, communicate, understand and certify the work that is performed by them (INCOSE, 2010). In order to measure the maturity of SOC services, industry-accepted maturity models will be used.

A SOC is much more than just the technology. People and processes form an integral part of a well-functioning SOC. From an operational effectiveness and efficiency perspective, we will use ITIL (Office of Government Commerce, 2000), CoBIT (ISACA, 1996; Adler, 2007) and ISO/IEC 27002:205 (ISO/IEC 27002:2005, 2009).

In this section, the processes and operational requirements will be aligned with the functional requirements. A policy will govern SOC operations. Policies will be written in commanding language and will include terms such as “must” and “will”. SOC policies will be supported by standards, processes and procedures. Service functions must be identified within the requirements. SOC service functions as derived from Bevis (2012) and Rothke (2009) are.

- Status Monitoring and Incident Detection;
- Initial Diagnostics and Incident Isolation;
- Problem Correction;

- Security Systems and Software (management of security technical controls);
- Computer equipment and end-point devices;
- Work with 3rd party vendors;
- Threat and vulnerability research and investigation; and
- Reporting.

These services can be broken down further, and will form the basis of process and procedure identification. Processes will typically flow from a policy, which governs operations. Bandor of the Software Engineering Institute (SEI) (Bandor, 2007) defines processes as the what that needs to be done, as well as the roles that are involved, and a procedure as the how of doing the task that is applicable to a single role. A process defines the roles and responsibilities of the staff that are assigned to execute a task, as well as the tools and equipment that are needed to do the tasks. Defining processes and procedures is important. It benefits the SOC service offering in that it improves communication and understanding. Areas of cost, quality, productivity and schedule are visible, and it aids in the planning process as well as the execution of plans. It also provides the basis for training and skills assessment, which is important for new SOC staff. It further ensures continuity and repeatability of SOC services.
A mapping of the SOC functional to the SOC service requirements are provided in Table 3-2.

Table 3-2: Mapping of SOC Service Functions to SOC Functional Requirements

Mapping of SOC Service Functions to SOC Functional Requirements	
Functional Requirements	**Service Requirements**
Event Log Collection and Management	
Real-time Monitoring, and analysis ability	Status Monitoring and Incident Detection
Incident Management	Status Monitoring and Incident Detection Initial Diagnostics and Incident Isolation Problem Correction
Reporting and visualisation	Reporting
Providing Strategic advice and guidance or Threat Intelligence	Threat and vulnerability research and investigation
Forensic and Investigative functionality	Threat and vulnerability research and investigation
Vulnerability Management	Threat and vulnerability research and investigation
Change Management	Security Systems and Software (management of security technical controls) Computer equipment and end-point devices
Network and Security Device Management	Security Systems and Software (management of security technical controls) Computer equipment and end-point devices Work with 3rd party vendors
Security Awareness Training	

The SOC functional requirements were determined in Section 3.2 by analysing vendor's descriptions of their SOC and MSSP service offerings in terms of functionality on offer. The SOC service functions were determined in section 3.3 by analysing SOC processes and policies as it appears in vendor literature. The SOC functional requirements are high-level requirements, and states the minimum functions an entity has to offer before it can be called a SOC. The service requirements are more detailed, and multiple SOC service requirements can be mapped back to SOC functional requirements. From this mapping, it can be seen that the majority of the SOC service functions can be mapped back to the incident management and operational aspects (network and security device management) of the functional requirements.

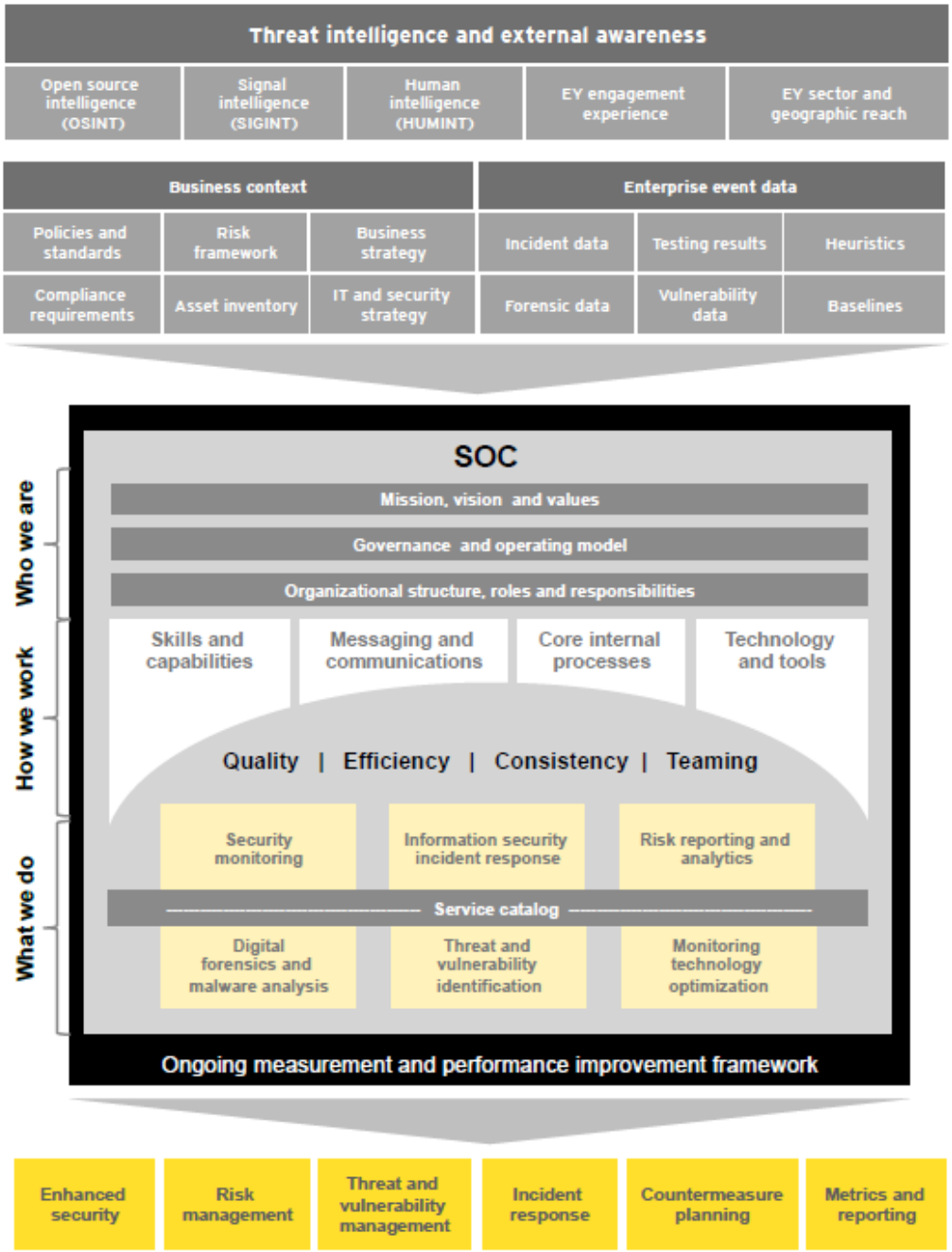

Figure 3-3: Sample SOC service architecture (Ernst and Young, 2013)

The SOC service functions are also supported by Ernst & Young, (2013), as depicted in Figure 3-3 Capabilities supporting the SOC service functions as listed by Ernst & Young are:

- Skills and capabilities corresponding to SOC people requirements
- Messaging and communication which corresponds to SOC functional requirements
- Core internal processes corresponding to SOC service and business requirements
- Technology and tools corresponding to SOC functional requirements

These enablers are further supported by the SOC mission, vision and values, governance and operating model and organisational roles, structures and responsibilities, with all these corresponding to SOC business requirements.

The service functions as listed by Ernst & Young are listed as follows in their service catalogue:

- Security monitoring corresponding to Real-time Monitoring, and analysis ability
- Information security incident response corresponding to Incident Management
- Risk reporting and analytics corresponding to Real-time Monitoring, and analysis ability
- Digital forensics and malware analysis corresponding to Forensic and Investigative functionality
- Threat and vulnerability identification corresponding to Vulnerability Management
- Monitoring technology optimisation corresponding to Event Log Collection and Management

A SOC needs policies, processes, procedures and standards to support it operations. There exists a relationship between policies, processes, procedures and standards. All these have to be developed keeping in mind the constraints, implementation parameters and supporting functions needed. The relationship between policies, standards, processes and procedures is shown in Figure 3-4.

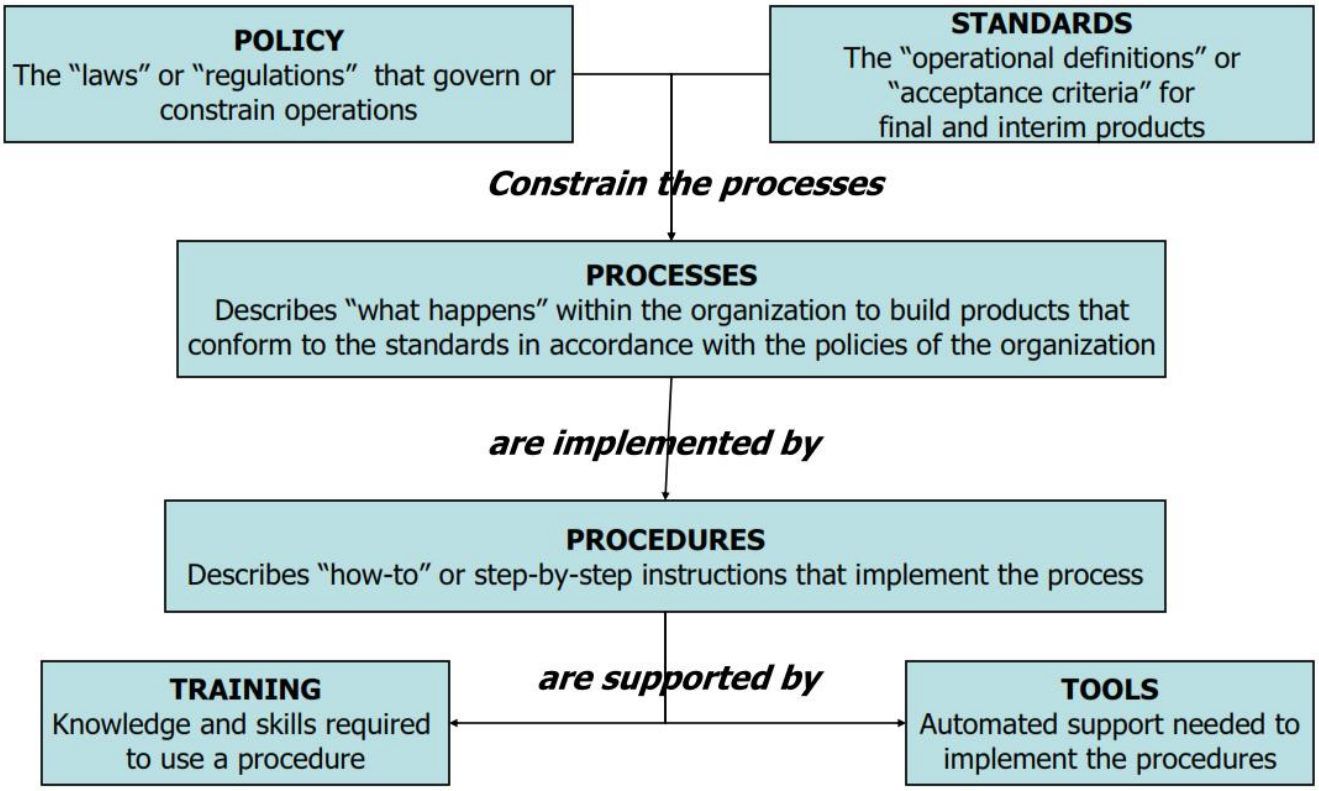

Figure 3-4: Relationship between Policies, Standards, Processes and Procedures (Bandor, 2007)

From the SOC service functions, a number of policies, processes and procedures are needed to ensure operational effectiveness, repeatability and continuity of services. Hardy *et al.,* (2008) aligned CoBIT 4.1 with ITIL V3 and ISO/IEC 27001:2005. CoBIT 4.1, The frameworks, standards and best practices used to develop the SOC framework are CoBIT 4.1, ITIL V3 and ISO/IEC 2001:2005, and these were used to determine the necessary policies and processes. The mapping of Hardy *et al.,* (2008) served as the basis, and was reproduced in Tables 3-2 to 3-8. The SOC service requirements as determined in section 3-3 were aligned and mapped back to the CoBIT 4.1, ITIL V3 and ISO/IEC 2001:2005 mapping done by Hardy *et al.,* (2008) The SOC service requirement mapping is presented in Tables 3-2 to 3-8. This rationale is to provide support for, and proof that the identified service requirements are valid, essential, and supported by the identified frameworks, standards and best practices.

Monitoring policy, process and procedure must be developed. The SOC environment must be monitored for anomalies or critical events. This could include monitoring for low disk space, malware on the SOC network and high CPU usage, which may indicate a malware outbreak or hacking attack. The SOC environment should be monitored just as rigorously as the client or organisation environment. Elements to be monitored should be clearly defined and documented. The monitoring requirements are listed in Table 3-3.

Table 3-3: Monitoring Policy, Process and Procedure Requirement (Hardy *et al.*, 2008)

Service Requirement	CobiT 4.1	ITIL V3 S	ISO/IEC 27001:2005
Status Monitoring and Incident Detection	DS13.3 IT infrastructure monitoring	• SD 4.3.5.4 The underpinning activities of capacity management • SD 4.3.5.5 Threshold management and control • SO 4.1 Event management • SO 4.1.5.1 Event occurs • SO 4.1.5.9 Review and actions • SO 5.2.1 Console management or operations bridge	• 10.1.1 Documented operating procedures • 10.7.4 Security of system documentation
	ME1.2 Definition and collection of monitoring data	SD 4.2.5.10 Complaints and compliments CSI 4.1c Step three—Gathering data CSI 4.1d Step four—Processing the data	• 10.10.2 Monitoring system use

Initial diagnostics, and Incident Management processes and procedures need to be developed. This will ensure that events with potential security implications are investigated, prioritised and escalated timeously or according to SLA or OLA. Sub-processes will include investigation processes, analysis processes, etc. The requirements are listed in Table 3-4.

Incident escalation process needs to be defined. This is a sub-process of the Incident Management Process. This will ensure that incidents are escalated timeously to the correct people, as agreed during the take-on or SLA with customer. The requirements are listed in Table 3-4.

Incident closure process needs to be developed. This is a sub-process of the Incident Management Process. After incidents have been resolved, they need to be closed. The root cause analysis needs to be done and added to the knowledge base. This could be done on a third party tool, or as part of the SIEM capabilities. The requirements are listed in Table 3-4.

Event and Incident classification process must be developed. This will allow SOC staff to correctly identify events that could have a security impact, classify the events in different severity levels and elevate the status to that of an incident, if necessary. This is a sub-process of the Incident Management Process. The requirements are listed in Table 3-4.

.

Table 3-4: Incident and Event Management Requirement (Hardy *et al*., 2008)

Service Requirement	CobiT 4.1	ITIL V3	ISO/IEC 27001:2005
Initial Diagnostics and Incident Isolation	DS8.1 Service desk	• SO 4.1 Event management • SO 4.2 Incident management • SO 6.2 Service desk	• 14.1.4 Business continuity planning framework
	DS8.3 Incident escalation	• SO 4.1.5.8 Response selection • SO 4.2.5.6 Incident escalation • SO 4.2.5.7 Investigation and diagnosis • SO 4.2.5.8 Resolution and recovery • SO 5.9 Desktop support	• 13.1.2 Reporting security weaknesses can be added as they pertain to event identification • 13.2.3 Collection of evidence • 14.1.1 Including information security in the business continuity management process • 14.1.4 Business continuity planning framework
	DS8.4 Incident closure DS10.1 Identification and classification of problems	• SO 4.1.5.10 Close event • SO 4.2.5.9 Incident closure • SO 4.4.5.1 Problem detection • SO 4.4.5.3 Problem categorisation	• 13.2.2 Learning from information security incidents • 13.2.3 Collection of evidence • 13.2.2 Learning from information security incidents

Change and Problem management process needs to be defined. This will be applicable to all IT equipment used in the SOC, as well as to the SIEM and its platform. Change management should also be followed when managing devices internally, or for customers. In a SOC Service provider scenario, the client's change management process will be followed. The requirements are listed in Table 3-5

Table 3-5: Problem Correction Requirement (Hardy *et al*., 2008)

Service Requirement	CobiT 4.1	ITIL V3	ISO/IEC 7001:2005
Problem Correction, Change and Patch Management	AI3.3 Infrastructure maintenance AI6.1 Change standards and procedures	• SO 5.4 Server management and support • SO 5.5 Network management • SO 5.7 Database administration • SO 5.8 Directory services management • SO 5.9 Desktop support • SO 5.10 Middleware management • SO 5.11 Internet/ web Management • SD 3.2 Balanced design • SD 3.7 The subsequent design activities • ST 3.2 Policies for service transition • ST 3.2.1 Define and implement a formal policy for service transition	• 9.1.5 Working in secure areas • 9.2.4 Equipment maintenance • 12.4.2 Protection of system test data • 12.5.2 Technical review of applications after operating system changes • 12.6.1 Control of technical vulnerabilities

Preventative Maintenance process must be developed. This is to ensure that the SOC equipment are regularly serviced and maintained so as to ensure optimum performance and to minimize impact due to overseen aspects. This should be done in accordance with the change management policy. The requirements are listed in Table 3-6.

Table 3-6: Preventative Maintenance Process Requirement (Hardy *et al.*, 2008)

Service Requirement	CobiT 4.1	ITIL V3	ISO/IEC 27001:2005
Security Systems and Software (management and maintenance of security technical controls) Computer equipment and end-point devices	DS13.5 Preventive maintenance for hardware	• SO 5.3 Mainframe management • SO 5.4 Server management and support	• 9.2.4 Equipment maintenance

A process for contacting, interacting and liaising with third parties needs to be established. This includes contact with threat intelligence service providers. The requirements are listed in Table 3-7.

Table 3-7: Third Party contacting Process Requirement (Hardy *et al.*, 2008)

Service Requirement	CobiT 4.1	ITIL V3	ISO/IEC 27001:2005
Work with 3rd party vendors	PO4.15 Relationships	• SD 4.2.5.9 Develop contracts and relationships	• 6.1.6 Contact with authorities• 6.1.7 Contact with special interest groups

Vulnerability management needs to be defined. This will be applicable to all IT equipment used in the SOC, as well as to the SIEM and its platform. Vulnerability management incorporates change and patch management. A vulnerability management strategy should be developed for the SOC. This is a signature-based approach to discover known vulnerabilities. Discovered vulnerabilities should be fixed to protect the SOC as well as the SOC network and assets from attacks that are exploiting known vulnerabilities. A well-run vulnerability strategy could also assist with asset discovery and classification. The requirements are listed in Table 3-8.

Table 3-8: Vulnerability Management Process Requirement (Hardy *et al.*, 2008)

Service Requirement	CobiT 4.1	ITIL V3	ISO/IEC 27001:2005
Threat and vulnerability research and investigation	12.6.1 Control of technical vulnerabilities	• AI3 Acquire and maintain technology infrastructure • AI6 Manage changes • DS5 Ensure systems security configuration	• SO 4.3.5.1 Menu selection • SO 4.3.5.3 Other approval • SO 4.5.5.6 Removing or restricting access • SO 5.13 Information security management and service operation

A Reporting capability and process needs to be defined. Reporting can be ad hoc, scheduled or on demand. It could be executed by the SOC, or in some instances made available to the client via a secure portal. This process should take the form of an SLA report to provide feedback on the number of incidents opened, the time taken to close them, the reasons for closing incidents late, trends etc. SOCs that are offering electronic Governance. Risk and Compliance (eGRC) service would be able to offer this as a service to clients. The mitigation and containment information regarding the incident, and whether or not there are any lessons learnt from the security incidents, should be captured and made available to staff and clients so as to allow them to learn form security incidents. The requirements are listed in Table 3-9.

Table 3-9: Reporting Capability and Process Requirement (Hardy *et al.*, 2008)

Service Requirement	CobiT 4.1	ITIL V3	ISO/IEC 27001:2005
Reporting	DS8.5 Reporting and trend analysis	• SO 4.1.5.9 Review and actions • CSI 4.3 Service measurement (vague)	• 13.2.2 Learning from information security incident

The SOC functional requirements, processes and procedures are listed in Appendix C.

In next chapters, these service requirements will be mapped back to the TM Forum's eTOM framework, with references back to the originating standard, framework or best practice.

Now that the SOC service functions, supported by CoBIT, ISO/IEC 27001:2005 and ITIL have been determined; the SOC people functions need to be determined. These will be derived from skills matrix compiled by CERT, and the management of the HR resources as required by CoBIT, ISO/IEC 27001:2005 and ITIL.

3.4 SOC People Functions

Staffing a SOC is a difficult task. One could have the latest cutting-edge technology and most comprehensive processes in place, but if the staff is not trained in the technology, or if they do not have sufficient skills to interpret the data, they cannot fulfil the tasks given to them and the SOC service will be degraded.

The most common mistake that organisations make when hiring SOC staff is that they do not get people with the right skills and experience (Combs, 2013; Ernst & Young, 2013). Good Cybersecurity skills are very scarce, which exacerbates the problem (Nakashima & Krebs, 2009; Evans & Reeder, 2010) The tendency is to start with too low a skill set for the SOC Analysts. Good analysts need trouble shooting skills, patience, research skills and the ability to communicate at different levels during times of stress (Arcsight, 2009).

SOCs need engineers with strong analytical skills, as well as with a solid knowledge of security in general and of the current landscape. They should have the ability to think fast, and know the technology with which they are monitoring as well as the technologies that they are monitoring. Experienced staff is hard to find, is expensive, and is also difficult to retain due to their wealth of knowledge and experience. It is therefore a necessity to define clear career paths (Broderick, 2007).

SOC staff should also be tiered. There must be a Level 1 Engineer responsible for the triage of incoming events, and a further layer (Level 2 to Level 3) with more experience, that are taking care of the more challenging incidents (Blake, 2012).

Depending on the SOC functions and mandate, operations may be over a 24/7 cycle. This will influence the number of engineers required to staff the SOC. Aspects to be kept in mind include a shift roster or staffing schedule, holiday coverage, shift logs, task lists and handover (Bevis, 2012). Staff should also be sent on training to provide them with job-specific skills to deal with security issues (Thanh Viet Do, 2003).

3.4.1 SOC Required Skills

Some vendor-specific and generic qualifications should also be included in the requirements, such as SANS GIAC GCIA certification, CISSP, CCNA, CCSP, CCSE and CCSA (Dell, 2013).

ISO/IEC 27001, CoBIT and ITIL also have human resources requirements, but these are from the perspective of securing the organisation against staff with malicious intent. The following controls are applicable to staff (Hardy *et al.,* 2008):

- Roles and Responsibilities must be established within the SOC;
- Prospective Employees should be properly screened before employment and

According to CERT (2003) and Milne (2005), staff should have the personal and basic technical skills that are detailed in Table 3-10:

Table 3-10: Proposed skills profile (Milne, 2005)

Personal Skills	Technical Skills
Communication, written and oral	Understanding of basic security principles such as access control, confidentiality, integrity, availability non-repudiation and privacy.
Presentation skills	Understand security vulnerabilities and weaknesses.
Diplomacy	Understand the Internet.
Ability to follow policies, processes and procedures	Understand network protocols.
Team skills	Understand network applications and services.
Integrity	Solid understanding of network security issues.
Coping with stress	Understanding of malicious code.
Problems solving skills	Programming skills in C, Perl, Java and shell scripting.
Knowing their limits	Incident management skills
Problem solving skills	Understanding policies, processes and procedures
Time management skills	Understanding and identifying intruder techniques

Terms and Conditions of employment should be explained to prospective employees, and they should sign off that they understand the terms and conditions.

Table 3-11: Employee Requirements (Hardy *et al*., 2008)

People Requirement	CobiT 4.1	ITIL V3	ISO/IEC 27001:2005
Human Resource Management	PO4.6 Establishment of roles and responsibilities	•SS 2.6 Functions and processes across the life cycle •SD 6.2 Activity analysis •SD 6.4 Roles and responsibilities •ST 6.3 Organisation models to support service transition •SO 6.6 Service operation roles and responsibilities •CSI 6 Organising for continual service improvement	•6.1.2 Information security co-ordination •6.1.3 Allocation of information security responsibilities •6.1.5 Confidentiality agreements •8.1.1 Roles and responsibilities •8.1.2 Screening •8.1.3 Terms and conditions of employment •8.2.2 Information security awareness, education and training •15.1.4 Data protection and privacy of personal information
	PO7.1 Personnel recruitment and retention		•8.1.1 Roles and responsibilities •8.1.2 Screening •8.1.3 Terms and conditions of employment

A Policy on the Acceptable use of Assets, as well as the return of Assets upon resignation needs to be created.

Table 3-12: Acceptable use and return of Assets Requirement (Hardy *et al.*, 2008)

People Requirement	CobiT 4.1	Key Areas	ITIL V3	ISO/IEC 27001:2005
Human Resource Management	PO6.2 Enterprise IT risk and control framework	• Promulgating and controlling policy • Alignment with enterprise risk and control		• 5.1.1 Information security policy document control framework • 6.2.2 Addressing security when dealing with customers • 7.1.3 Acceptable use of assets • 8.2.2 Information security awareness, education and training • 8.3.2 Return of assets • 9.1.5 Working in secure areas • 9.2.7 Removal of property • 10.7.3 Information handling procedures • 10.8.1 Information exchange policies and procedures • 10.9.3 Publicly available information • 11.1.1 Access control policy of personal information
	PO7.8 Job Change and termination	• Knowledge transfer and reassignment so as to minimise risks		• 8.2.3 Disciplinary procedures • 8.3.1 Termination responsibilities • 8.3.2 Return of assets

3.5 Summary

In this chapter we have used System Engineering principles to determine the requirements of a SOC. These are:

- SOC Functional Requirements which describes the core functions a SOC should provide;
- SOC Service Requirements; which describes the minimum critical services a SOC should provide and
- SOC People Requirements that describes aspects related to the staffing of a SOC, such as skills, qualifications and attributes SOC staff should have.

These requirements were then mapped back to ISO/IEC 27001:2005, CoBIT and ITIL.

The service requirements are also supported and confirmed by Allen (2003).

In Chapter 4, the outputs of Chapter 3 are mapped back to the eTOM Process Framework. Business processes not covered by ISO/IEC 27001:2005, CoBIT and ITIL are identified and included. Table 3-13 provides a consolidated view of the requirements mapped back to their most suitable framework or standard.

Table 3-13: Consolidated requirements mapping

	Etom	ITIL	CoBIT	ISO 27002
SOC Primary Functional Requirements				
Event Log Collection			●	
Event Log Management				●
Real-time Monitoring			●	
Analysis ability	●			
Incident Management		●		
Reporting and visualisation				●
Provide Strategic advice and guidance				●
Threat Intelligence				●
Forensic and Investigative functionality	●			
Vulnerability Management				●
Business Impact Assessment			●	
Change Management		●		
Network and Security Device Management			●	
Security Awareness Training				●
SOC Service Requirements				
Status Monitoring and Incident Detection			●	
Initial Diagnostics and Incident Isolation		●		
Problem Correction		●		
Security Systems and Software (management of security technical controls)				●
Computer equipment and end-point devices				●
Work with 3rd party vendors				●
Threat and vulnerability research and investigation				●
Reporting			●	
SOC Business Requirements				
Market and Strategy Policy	●			
Product and Offer Portfolio Planning	●			
Product and Offer Capability Delivery	●			
Product and Offer development and Retirement	●			
Sales Development	●			
Product Marketing Communications and Promotion	●			
Service Strategy and Planning	●			
Service Capability Delivery	●			
Customer Relationship Management	●			
Service Management and Operations	●			
Resource Performance Management	●			
Workforce Management	●			
Supplier / Partner Relationship Management	●			
Strategic and Enterprise Planning				●
Enterprise Risk Management	●			
Financial and Asset Management	●			
Stakeholder and External Relations Management	●			
Human Resources Management	●			

4 SOC Business Requirements

4.1 Introduction

In Chapter 3, the SOC functional, service and people requirements were determined. In this chapter, we will be determining the SOC business requirements using the TM Forum's eTOM framework. These are all the business-related requirements that are not covered by the functional and service requirements.

For the purpose of creating a Security Operation Center business framework, we will be using the TM Forum's Business Process Framework (eTOM), *"which is a comprehensive, industry-agreed multi-layered view of the key business processes that are required to create and run a business"* (TMForum, 2013). Use of the eTOM Business Process Framework will allow for the use of a common language by means of which to understand, design, develop and manage IT Services in terms of business requirements, and to identify opportunities to improve performance and cost.

The functional and service requirements determined in Chapter 3 will be compared against the eTOM framework and, where necessary, augmented with ITIL, ISO/IEC 27001:2005, and CoBIT. The Business Process Framework consists of three business concepts, which can be broken down into three (3) levels. These are Strategy, Infrastructure and Product (Level 0), Operations (Level 0) and Enterprise Management (Level 0). Only processes applicable to Security Operation Centers will be identified and used as part of the framework (TMForum, 2013). The eTOM framework consist of three main sections, these sections are Strategy, Infrastructure and Product, Operations and Enterprise Management. Within the Strategy, Infrastructure and Product, and Operations sections, vertical process views exist, with horizontal process functions. This illustrated in Figure 4-1 as taken from TMForum (2013). Layer 2 is further broken down into Layer 3, 4 and 5processes.

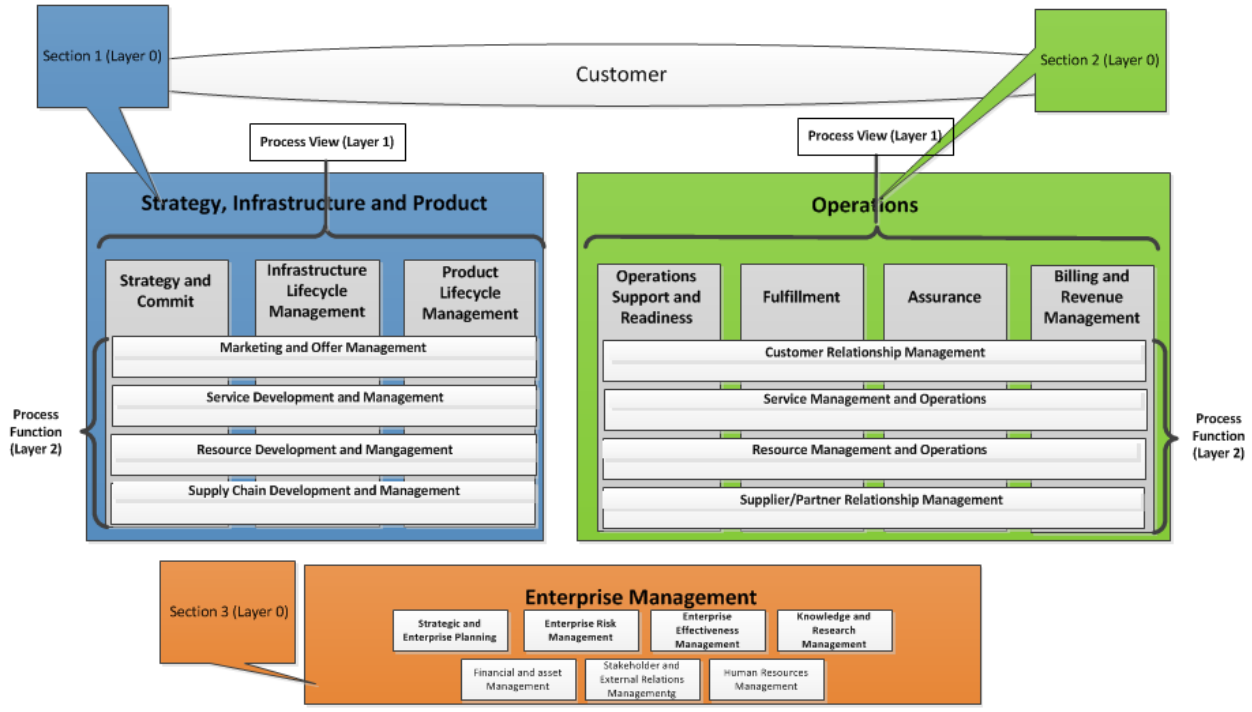

Figure 4-1: eTOM layout

The horizontal layers are Level 2 processes, and two are mentioned – along with their child processes by way of illustration:

- Strategy, Infrastructure and Product (Layer 0) with Strategy and Commit (Layer 1) Marketing and Offer Management as Layer 2; Market Strategy and Policy as Layer 3 and Establish Market Strategy as Layer 4, with Support Market Strategy as Layer 5
- Operations (Layer 0) with Fulfilment (Layer 1), and Customer Relationship Management as Layer 2, Bill Invoice Management as Layer 3, Create Customer Bill Invoice as Layer 4, and Deliver Electronic Invoice as Layer 5

The hierarchy is illustrated in Figure 4-2:

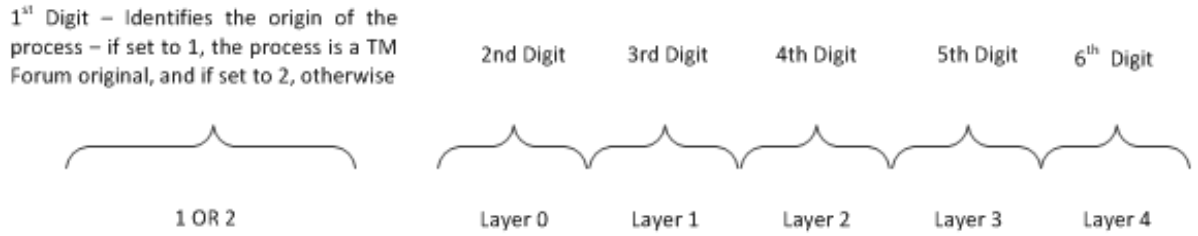

Figure 4-2: TM Forum numbering scheme (TMForum, 2013)

Each child process is identified by a unique identifier, which can be used to locate the process.

This approach will provide us with a complete framework, covering functional and service requirements, that was determined using Systems Engineering principles and then mapped back to CoBIT, ITIL and ISO/IEC 27001:2005. It also includes business requirements that were determined using the eTOM framework.

At the end of the chapter the functional, service and business requirements are consolidated into one framework.

In the TMFoum eTOM framework, Enterprise Management focuses on the internal management of an organisation. This will be applicable to SOCs. The processes applicable to SOCs will differ with respect to the business model that is followed. A SOC could be seen as part of a business with a shared cost center, or as a business unit on its own with its own cost center.

Strategy, Infrastructure and Product as well as Operations are focused outwards, and addresses the services offered by an organisation to its clients. These are elements that are seen by the customer, which could be either internal or external. These processes will be applicable to a SOC seen as delivering a service to the organisation, with Operation Level Agreements and robust governance requirements. SOCs can also offer a service to clients, and as such need to have a sales strategy and sales plan, a service catalogue and a sales capability, to name but a few. The eTOM process framework is illustrated in Figure 4-3

The people, processes and technology approach excludes elements such as facilities, marketing and sales strategy, and business plans. These will be addressed separately, as part of the eTOM framework.

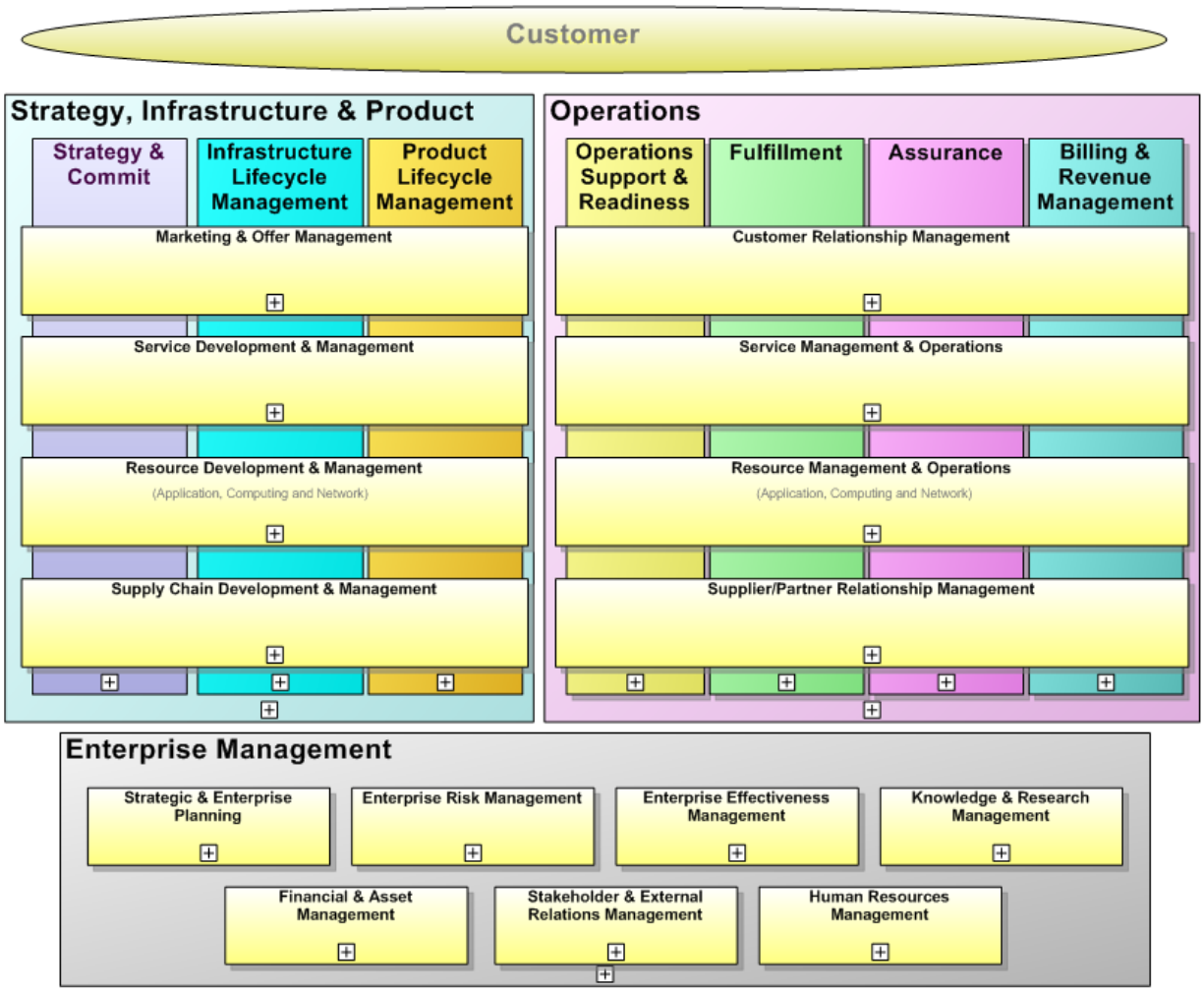

Figure 4-3: TM Forum Business Process Framework (TMForum, 2013)

In the following section business requirements are identified using the eTOM business process framework as depicted in Figure 4-2, with a rationale on why the selected processes are applicable to SOCs. During this research, limited reference or material addressing SOC business requirements could be found, and as a result no reference exists to map these requirements back to.

4.2 Strategy, Infrastructure and Product

This section covers the planning and lifecycle management of a product or service.

From a **Strategy, Infrastructure and Product** perspective, the following processes are applicable to Marketing and Offer Management. Figure 4-4 shows context where Strategy, Infrastructure and Product fit into the eTOM framework. The Strategy, Infrastructure and Product area is highlighted in blue. Market and Strategy Policy is highlighted in red. Figures 4-4 to 4-18 are not meant to be read, but indicate the position with the eTOM framework.

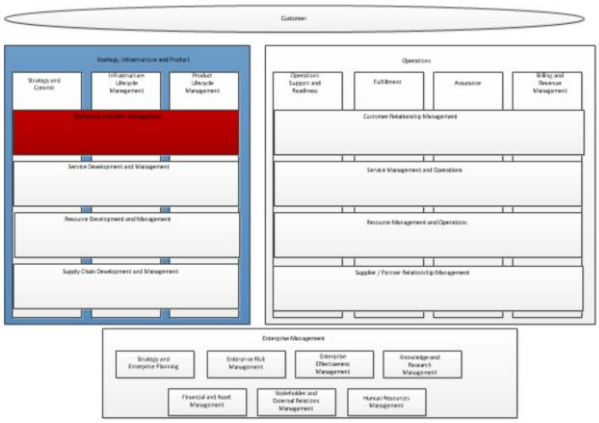

Figure 4-4: Marketing and Offer Management

Market and Strategy Policy (1.2.1.1)

- Gather and Analyse Market Information (1.2.1.1.1)

  The establishment and management of relationships with external providers of market information, as well as the management of internal resources that are used to provide market information, takes place here (TMForum, 2013).

  From a SOC perspective, market research needs to be done and forecasts must be developed before applying internally for finance. Internal SOC solutions must also be marketed internally to the business.

Product and Offer Portfolio Planning (1.2.1.2)

- Gather and Analyse Product Information (1.2.1.2.1)

  Research should be done regarding product ideas and opportunities, and product opportunities should be identified (TMForum, 2013).

  - Gather Product Information

    Internal and external resources should be researched and analysed in order to identify new products as well as to review existing products.

    SOCs should keep abreast of new capabilities of technologies such as SIEM's, which will enable them to provide a better or more comprehensive service to the organisation.

    This includes new and emerging technologies such as anomaly detection and the capability of some Unified Threat Management (UTM) technologies to provide Security as a Service (Secaas), using policy-based routing.

Product and Offer Capability Delivery (1.2.1.3)

- Define Product Capability Requirements (1.2.1.3.1)

  This defines and obtains agreement on the infrastructure that is required to support the product or service portfolio.

  - Capture Product Infrastructure Requirements (1.2.1.3.1.1)

The Define Product Capability Requirements process defines the detailed infrastructure requirements for supporting the product or service portfolio, both currently and in future. It also identifies the service infrastructure capabilities that are required to deliver the product or service (TMForum, 2013).

SOCs need to define supporting infrastructure. This includes Information Technology, facilities, lighting, access control, etc. This process can further be supported by standards such as ISO/IEC 27001:2005, or legal requirements. This will also define SLAs and support elements from suppliers and vendors.

- Approve Product Business Case (1.2.1.3.3)

  The Approve Product Business Case process captures all the activities that are required in order to develop a business case for the development and delivery of the required capabilities. This includes identification of potential partners or suppliers. Required product infrastructure components, development cost and anticipated benefits should also be captured as part of this process (TMForum, 2013).

  - Develop Product Business Case (1.2.1.3.3.1)

    As part of the planning of building a SOC, a product business case should be developed. Technology vendors need to be identified. Partnerships should be established with organisations that are supplying threat intelligence and supplementary services to the SOC.

  - Gain Product Business Case approval (1.2.1.3.3.2)

    This process includes all the activities that are required to gain the necessary approval for a business case for the development and delivery of the required capabilities (TMForum, 2013).

    Commitment by management is extremely important. SOCs cost money, and management needs to approve the initiative and make funds available. This is applicable to all SOCs. It also includes the development of new services and the procurement of components that are required to provide and deliver the service. Without management commitment and the necessary funding, SOC projects are doomed to fail.

- Deliver Product Capability (1.2.1.3.4)

  The Deliver Product Capability process manages the co-ordinated delivery of required product infrastructure capabilities of the business case (TMForum, 2013).

  This process ensures that the delivery of supporting capabilities such as facilities, technology and staff takes place to provide the SOC services.

Product and Offer Development and Retirement (1.2.1.5)

The Product and Offer Development and Retirement process defines the development and delivery of new products, service enhancements and features for implementation by the operational process.

- Gather and Analyse new Product Ideas (1.2.1.5.1)

  The Gather and Analyse new Product Ideas process addresses the research and analysis of demographic, customer, technology and marketing information to identify new product and service opportunities (TMForum, 2013).

  - Identify Opportunities and Requirements (1.2.1.5.1.2)

    The Identify Opportunities and Requirements process identifies potential opportunities, as well as requirements from the sales function regarding improvement on current product or service offerings (TMForum, 2013).

    In order to stay competitive, SOCs should constantly identify and offer new services. These could involve small changes such as shortening response times, or big changes such as offering Governance Risk and Compliance dashboards to customers. Internal SOCs should improve on their services to the organisation by utilising new technologies to improve the security posture of their organisation.

  - Develop New Product Business Proposal (1.2.1.5.3)

    Business proposals are developed for the newly identified opportunities (TMForum, 2013).

    New opportunities for SOCs will in most cases have a financial impact. Examples are the acquisition of additional storage or additional technologies currently not deployed within the SOC. For this purpose, a business proposal needs to be developed, and supported and signed off by management.

  - Develop Product Commercialisation Strategy (1.2.1.5.4)

    The Develop Product Commercialisation Strategy process assures that the service pricing, sales channel support (brochures and marketing material) and regulatory approvals are identified and adhered to. It ensures that all sales support features are developed (TMForum, 2013).

    SOCs should market new capabilities and offerings, and should provide pricing and marketing information to the sales function.

Sales Development (1.2.1.6)

- Develop Sales and Channel Proposals (1.2.1.6.2)

  The Develop Sales and Channel Proposals process creates and documents proposals for the sales function (TMForum, 2013).

  SOCs should develop sales proposals to assist the effectiveness of the sales function.

Product Marketing Communications and Promotion (1.2.1.7)

- Develop Product and Campaign Message (1.2.1.7.2)

  The Develop Product and Campaign Message process manages all activities and stakeholder engagements to develop a specific campaign (TMForum, 2013).

For a new SOC start-up, this will form an important process in the creation of awareness and in marketing of the new offering.

In Figure 4-5, Service Strategy and Planning is highlighted in red in the eTOM contextual figure. From a Service Development and Management perspective, the following processes are applicable to SOC:

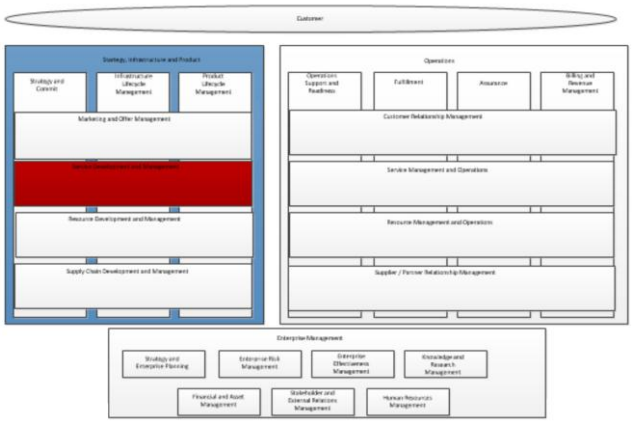

Figure 4-5 Service Development and Management

Service Strategy and Planning (1.2.2.1)

- Establish Service Strategy and Goals (1.2.2.1.3)

  The Establish Service Strategy and Goals process is to establish the service strategy based on market trends, future products, needs, and technical capabilities. It also addresses shortcomings in existing service performance and support (TMForum, 2013).

  - Establish and Develop Service Strategy (1.2.2.1.3.1 and 1.2.2.1.3.2)

    SOC services are constantly changing as new technologies and capabilities are released. The threat landscape also constantly changes, and SOC service providers should be geared to effectively confront any new threat with either new technologies or new techniques. It is therefore important that SOCs keep abreast of new market trends such as the need to provide session-based instead of packet-based monitoring to allow for better forensic capabilities.

  - Define Service Support Strategies (1.2.2.1.4)

    The Define Service Support Strategies process defines the principles, policies and performance standards for the operational organisation that is providing service support (TMForum, 2013).

    SOCs would have guaranteed services and Service Level Agreements (SLAs) with clients. Before clients can sign up for SOC services, they have to know what they are paying for, and what the performance measurements are. They also need to know what service levels and quality to expect from the SOC.

Service Capability Delivery (1.2.2.2.6)

- Enable Service Support and Operations (1.2.2.2.5)

The Enable Service Support and Operations process manages the provisioning, implementation and rollout of the new or enhanced service capability. It also manages the design improvements or changes that are required for the operational support of the service (TMForum, 2013).

SOCs offer a service that needs to be managed. These services can differ, ranging from monitoring and incident management to management of security technical controls. The provisioning as well as the delivery of these services needs to be managed properly. Considerations are the completion of take-on documents, the transfer of data from the client to the SOC, etc.

- Identify Service Support groups, Skills and Training (1.2.2.2.5.2)

  The Identify Service Support groups, Skills and Training process focuses on the identification of support groups or staff, their required skills sets, as well as the availability of appropriate training programs (TMForum, 2013).

  It is very difficult to get well-trained and experienced staff to operate a SOC and to provide support to managed devices and supporting technology. It is therefore important to identify all these issues upfront, in order to ensure that the correct people are appointed and that training of the technologies that are used is readily available.

- Identify Service Support Requirements (1.2.2.2.5.3)

  The Identify Service Support Requirements process ensures the identification, collation and co-ordination of support requirements from all approved investment proposals. Support shortfalls will also be identified in this process (TMForum, 2013).

  The type of services offered by SOCs, as well as the criticality of the service coupled with legal and other governance requirements, might mandate different support levels, maintenance contracts and repair SLAs. This addresses issues such as downtime from technology failure, etc.

Figure 4-6 contextualises the position of the Resource Development and Management container within the eTOM framework. From a Resource Development and Management perspective, the following processes are applicable to SOC:

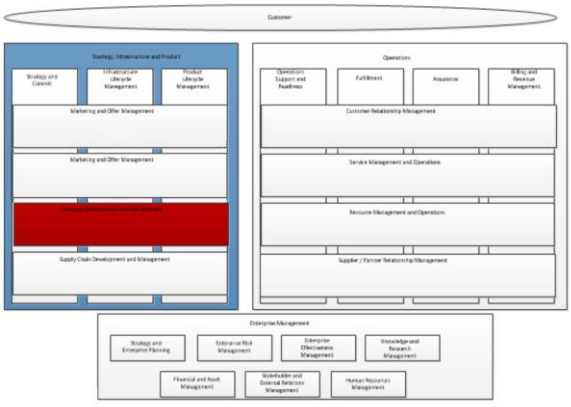

Figure 4-6: Resource Development and Management

The Resource Development and Management processes target the resource function of an organisation. These processes include aspects such as the planning, developing and delivering of resources needed in support of the services and products residing in the Operations domain. These processes address resources - both physical such as technologies, and non-physical such as management of current resources and ensuring that resources requirements meet future demand. (TMForum, 2013). There are no business processes applicable to a SOC in the Resource Development and Management horizontal functional container. Processes applicable to the operational domain is addressed by ITIL.

From a Supply Chain Development and Management perspective, the processes are applicable to SOC are shown in Figure 4-7.

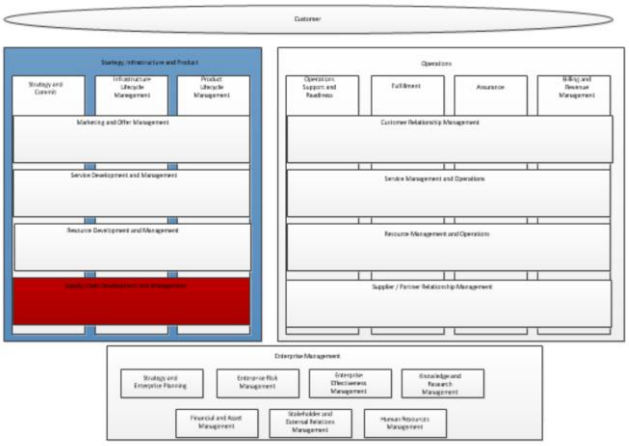

Figure 4-7: Supply Chain Development and Management

The target of the Supply Chain Development and Management process is the synergy between suppliers and partners to organisations in support of the supply chain maintenance. This is typically an intricate network of relationships that needs to be managed by the service provider in order to find and provide products. Selecting the optimum suppliers and partners is the aim of this process. It furthermore supports sourcing decisions made by the organisation, and ensures that the capabilities are in place for cooperation between the organisation, its suppliers and partners. It also ensures timeliness in terms of delivery of support, and that there are mechanisms in place to measure the effectiveness and performance of the partners and suppliers.

Another key function of the Supply Chain Development and Management process is to put mechanisms in place to capture, provide and maintain all the information and financial flows between the provider the organisation and the supplier (TMForum, 2013). There are no business processes applicable to a SOC in the Supply Chain Development and Management horizontal functional process since supplier and partner relationships as well as SLA management are addressed by CoBIT, ITIL and ISO/IEC 27001:2005.

In this section, the Strategy, Infrastructure and Product and Operations business processes, which are customer-facing processes, have been identified. In the next section, the Enterprise Management business processes, which are internal processes, will be identified.

4.3 Operations

This section covers the core day-to-day operational management in support of a product or service. The position of Operations within the eTOM framework is shown in Figure 4-8, and is highlighted in green. Customer Relationship Management is highlighted in red.

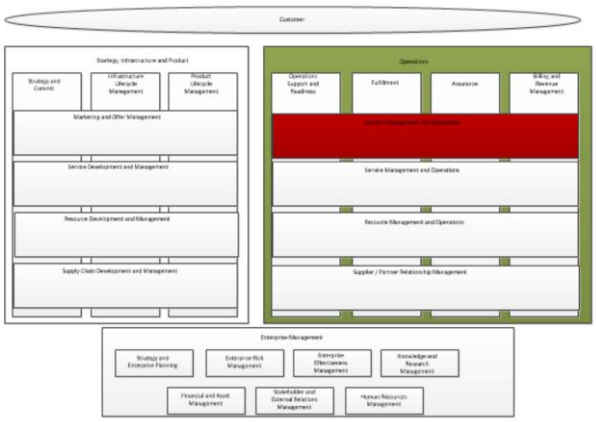

Figure 4-8: Customer Relationship Management

From an Operations and Customer Relationship Management perspective, the following processes are applicable to SOC:

Customer Relationship Management

- Bill Invoice Management (1.1.1.10)

  The Bill Invoice Management process ensures that all information, systems, material and resources are available so as to enable completion of the invoice management without delay. This includes information that is required to invoice clients, such as metering and back-billing information in the case of virus outbreak (if the costing model is events-per-second based) (TMForum, 2013).

  - Apply Pricing, Discounting, Adjustments and Rebates (1.1.1.8.2)

    The Apply Pricing, Discounting, Adjustments and Rebates process ensures that the customer receives an invoice that is reflective of all billable events. It also ensures that all discounts and rebates are applied to invoices (TMForum, 2013).

    This process ensures that a proper billing management process is followed. Different SOCs will use different costing models, such as events per second, a percentage of the cost of devices monitored, billing per remote collector, or SLA-based billing. This implies some sort of measuring or metering system. Where SOCs manage security technical controls, these will also have to be included. One model could be where clients buy an amount of hours per month (non-accumulative), or device management can be SLA-driven. Overtime and after-hours also have to be taken into consideration. SOCs need to collect this information and make it available to the financial department.

  - Create Customer Bill Invoice (1.1.1.10.2)

The purpose of the Create Customer Bill Invoice process is to create timely and accurate invoices in accordance with billing cycles. It should be reflective of the final charges for services (TMForum, 2013).

A mechanism or capability needs to exist for SOCs to generate invoices and distribute those to clients. This includes the capability to render or format invoices, as well as a way of storing the invoices for a specific period of time as required by regulatory, client or internal requirements.

- Produce and Distribute Bill (1.1.1.10.3)

  The Produce and Distribute Bill process addresses the physical production and distribution of bills to customers (TMForum, 2013).

  A mechanism for the production and distribution of bills to customers' needs to exist for SOCs. Distribution could be physical or electronic.

- Selling (1.1.1.4)

  The purpose of the Selling process is twofold: to administer and manage the operations of sales channels, and also to ensure that there is capability such as material, systems and resources to support the sales cycle (TMForum, 2013).

  SOCs should ensure that they have collateral available to support the sales process. This includes proposals, a pre-sales capability, presentations, pricing information and other documents. Internal SOCs still have to make businesses aware of their capabilities and offerings.

  - Develop Sales Proposal (1.1.1.4.6)

    The Develop Sales Proposal process supports the development of sales proposals to respond to the customer's needs. The development of the sales proposal may require the development of a non-standard offering, or the selection of a standard offering (TMForum, 2013).

    SOCs should have the capability to develop proposals, and should be flexible when developing their proposals. They should understand the customer's needs, and develop the proposal around the fulfilment of those needs. Even though it is advisable to have standard offerings, flexibility might give one SOC an advantage over a second, non-flexible SOC.

- Problem Handling (1.1.1.6)

  The Problem Handling process facilitates the management and resolution of problems reported by customers. The aim of this process is to ensure a mechanism is in place to facilitate the receipt of reports from customers, as well the redress of the problem to the customer's satisfaction. (TMForum, 2013).

  SOCs should be able to capture, analyse, manage and report on problems experienced by customers. They must further be able to assign problems to resolvers, correct the problem and assign and track problems.

- Customer QoS/SLA Management (1.1.1.7)

The Customer QoS/SLA Management process manages all interfaces between the SOC and customers. This includes reception and recording of contracts, directing of inquiries to the correct processes, monitoring and controlling the status of inquiries and escalation where necessary, and ensuring a consistent image (TMForum, 2013).

SOCs might decide to sell their services as an SLA. The SLA needs to be managed to ensure that there are no breaches against it, and that the customer gets what he pays for. This includes items such as incident management response times, penalties and other parameters. Internally, SOCs may have an Operational Level Agreement (OLA) in place with internal business units, and this needs to be managed just as carefully.

Service Management and Operations is contextualised in red in Figure 4-9.

From an Operations and Service Management perspective, the following processes are applicable to SOC:

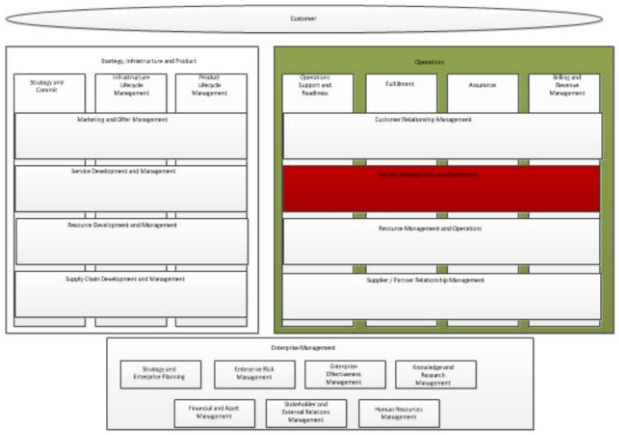

Figure 4-9: Service Management and Operations

Service Management and Operations (1.1.2)

- SMO Support and Readiness (1.1.2.1)
    - Manage Service Inventory (1.1.2.1.1)

      The Manage Service Inventory process manages, establishes and administers the services inventory and monitors and reports on the usage of, and access to, the service inventory (TMForum, 2013).

      SOCs must have a service catalogue that is kept up to date. The catalogue will describe all services, with clear deliverables and measurements of the effectiveness of the services. This will be used during the sales cycle as well. SOCs should have something similar to introduce their services internally, as well as to create a clear distinction of its roles and responsibilities relative other operational monitoring and management services in the organisation such as the Network Operations Center (NOC).

    - Support Service Problem Management (1.1.2.1.3)

The Support Service Problem Management processes have two focus areas. The first purpose is the assistance provided to the Service Problem Management processes by providing preventative and scheduled maintenance activities applicable to the infrastructure, and secondly it facilitates the monitoring, management and reporting of the Service Problem Management processes capabilities. (TMForum, 2013).

These processes are responsible for ensuring that the service infrastructure is working effectively and efficiently.

Responsibilities of these processes include, but are not limited to as paraphrased from TMForum, (2013):

- Extracting and analysing data, including trend analysis, historical and current service instance problem reports and performance reports, to identify potential service infrastructure or service instances requiring proactive maintenance and/or replacement;
- Requesting scheduling of additional service instance data collection to assist in the analysis activity;
- Requesting scheduling of service instance performance testing to assist in the analysis activity;
- Developing and managing service infrastructure and service instance proactive maintenance programs;
- Requesting service provisioning activities to prevent anticipated service problems associated with capacity limitations, as identified in the analysis activities;
- Reporting the outcomes of trend analysis to Service Development & Management processes in order to influence new and/or modified service infrastructure development;
- Tracking and monitoring of the Service Problem Management processes and their associated costs (including where service infrastructure is deployed and managed by third parties), and reporting on the capability of the Service Problem Management processes; and
- Establishing and managing service problem notification facilities and lists to support the Service Problem Management notification and reporting processes.

SOCs must have measures in place to ensure continuity of their services. With this in mind, regular maintenance should be done on all technology infrastructure that supports the services function. This will ensure that SOCs are scalable and can grow on demand and in line with customer requirements. This process includes concepts such as capacity management, patch- and vulnerability management and performance management.

- Service Quality Management (1.1.2.4)

The Service Quality Management process addresses the management, tracking, monitoring, analysis, improvement of (and reporting on) the performance of specific services (TMForum, 2013).

- Monitor Service Quality (1.1.2.4.1)

The Monitor Service Quality process is responsible to, through monitoring and logging, collect and detect service-specific quality data (TMForum, 2013).

SOCs need to have a capability in place that enables them to collect and log service-related information. This could include trending, baseline deviations and other anomalies in service performance. These anomalies need to be reported on, and must be remediated. This goes for traditional SOC monitoring services, as well as for management of technical security controls, mitigation and remediation services, governance, risk and compliance services and anomaly-based detection services. The same applies in equal measures to internal SOCs. Service offerings also need to be improved on if necessary, and must be reported on.

Resource Management and Operations is contextualised in Figure 4-10.

From a Resource Management and Operations perspective, the following processes are applicable to a SOC:

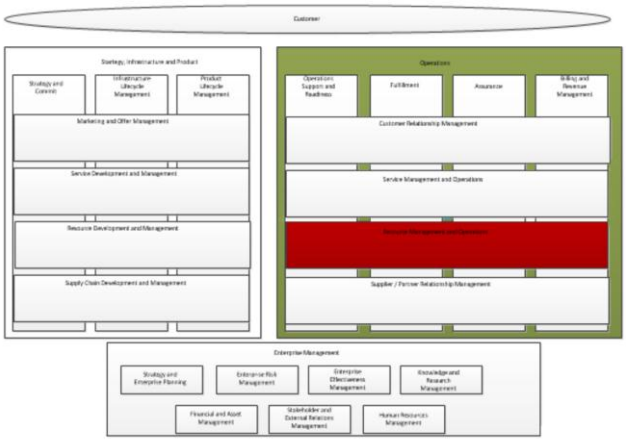

Figure 4-10: Resource Management and Operations

Resource Performance Management (1.1.3.4)

- Monitor Resource Performance (1.1.3.4.1)

  The Monitor Resource Performance process monitors received resource performance information and undertakes first detection (TMForum, 2013).

  SOCs must constantly monitor the performance of their SIEM. This will ensure that they do not run out of capacity in the case of malware outbreaks or attacks. Disk usage, CPU usage and other parameters should constantly be monitored, and alerts should be sent to appointed resources to manage the situation.

- Control Resource Performance (1.1.3.4.3)

  The purpose of the Control Resource Performance process is to apply controls to resource instances in order to perform resource performance (TMForum, 2013).

  Once resource-monitoring information has become available, SOCs should apply controls, whether technical or administrative, to resources. This could include controls such as limiting the time during the day when bandwidth can be used for personal usage, or the addition of extra storage.

- Workforce Management (1.1.3.7)
    - Manage Schedules and Appointments (1.1.3.7.1)

      The Manage Schedules and Appointments process manages the availability of staff, as well as the ability to schedule them.

        - Determine Work Schedule (1.1.3.7.1.2)

          The Determine Work Schedule process manages the available work capacity for a given time slot (TMForum, 2013).

          SOCs must manage their staff, as well as staff availability. This is done using shift rosters, leave planning and study leave schedules. SOCs typically offer 24x7 monitoring and staff needs to be available for shifts, as well as for standby. From a device management perspective, it is important to have the right staff with the right skills available to fulfil customer requirements for specific periods.

The Supplier Partner Relationship Management position within the eTOM framework is contextualised in Figure 4-11.

From a Supplier/Partner Relationship Management perspective, the following processes are applicable to SOC:

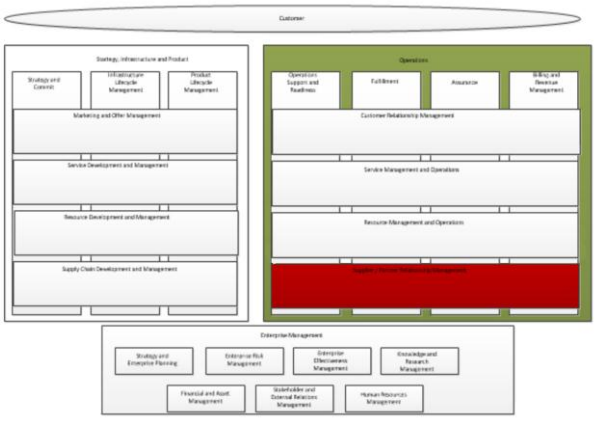

Figure 4-11: Supplier/Partner Relationship Management

Supplier/Partner Relationship Management (1.1.4)

- Supplier/Partner Problem Reporting and Management (1.1.4.3)

  The Supplier/Partner Problem Reporting and Management process tracks, monitors and reports on the service provider-initiated problem engagement (TMForum, 2013).

  SOCs must have a way of monitoring the status of resolution of reported problems, and feeding it back to the client.

4.4 Enterprise Management

This section covers corporate or business support management. The position of Enterprise Management in the eTOM framework as well as Strategic and Enterprise Planning is contextualised in Figure 4-12. From an Enterprise Management perspective, the following processes are applicable to SOC:

Strategic and Enterprise Planning (1.3.1)

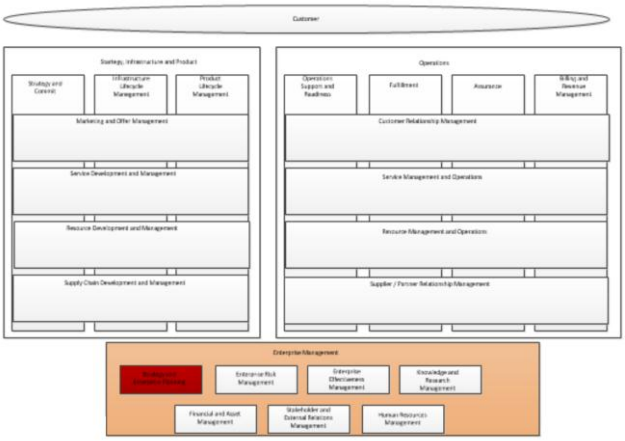

Figure 4-12: Enterprise Management - Strategic and Enterprise Planning

- Strategic Business Planning (1.3.1.1)

  The Strategic Business Planning process aim is to facilitate the provisioning of strategic business direction to the organisation. It is inclusive of all required functions to provide strategic business direction. It also assist the organisation in creating actionable plans, as well as providing high-level project management of the strategy implementation. (TMForum, 2013).

  This is an important process during the establishment of a SOC, since the business plan will show intent by sponsors to build and staff the SOC. This will also provide the business case and initial requirements for the SOC. During this process, the product and service will be defined. The same holds true for internal SOCs. A business case has to be made for the building and staffing of a SOC, even if it is for internal consumption.

- Business Development (1.3.1.2)

  The Business Development process develops the concepts for new revenue streams, as well as for the diversification of revenue streams (TMForum, 2013).

  - Develop Concepts for Revenue Streams (1.3.1.2.1)

    The focus of this process is to broaden the enterprise (SOC) activities through expansion.

    This process is applicable to SOCs. In order to stay competitive, SOCs will have to diversify and introduce new services, and build new capabilities. For example, a SOC could expand to offering Secaas complementing its monitoring and management services. With technology, SLA incident response times can

be guaranteed at ten minutes, providing the customer with a portal to allow him to generate on-demand reports, etc.

- Group Enterprise Management (1.3.1.4)

  The Group Enterprise Management process is responsible for the planning and management of co-ordination across business units, as well as across the enterprise and its subsidiaries (TMForum, 2013).

  - Plan and Implement Cross-Business Unit Operation (1.3.1.4.1)

    Internally, SOCs need to manage and co-ordinate across all business units within the organisation. This typically implies the NOC (if there is one), Operations, the patch management team, Human Resources, etc. SOCs as a business entity will need to interact with client organisations. In order to provide a professional service, SOCs need to understand aspects such as the client environment, its IT Operations, the change management process, Finance, etc.

- ITIL Change Management (1.3.1.6)

  ITIL Change Management optimizes risk exposure, minimizes business disruptions and ensures that everything related to the live- or production environment goes right the first time. It also ensures that all changes to the IT environment are assessed and executed in a controlled manner (TMForum, 2013).

  For SOCs this is important during the take-on process, where change needs to be made to the IT environment of clients. This could range from the installation of an appliance to the installation of an agent, or reconfiguration of monitored devices. In the case of SOCs that are managing security technical controls for clients, all changes to these devices need to be managed via change processes.
  It is also important for Internal SOCs, where changes need to be made to monitored and managed devices. With SOC service providers the focus would mostly be outward facing, and they would have to adhere to change control processes and philosophies of multiple clients. In contrast, internal SOCs mostly only have to focus on their organisation's change control processes.

Enterprise Risk Management (1.3.2)

The Enterprise Risk Management position in the eTOM framework is contextualised in Figure 4-13.

- Business Continuity Management (1.3.2.1)

  The main focus of the Business Continuity Management process is to ensure the continuity of organisational processes in the event of severe and continuous interruption to business processes, or the ability of an organisation to conduct business. It achieves this by identifying roles and responsibilities, plans and escalation procedures. It also determines that the continuity plans be established and regularly tested. (TMForum, 2013).

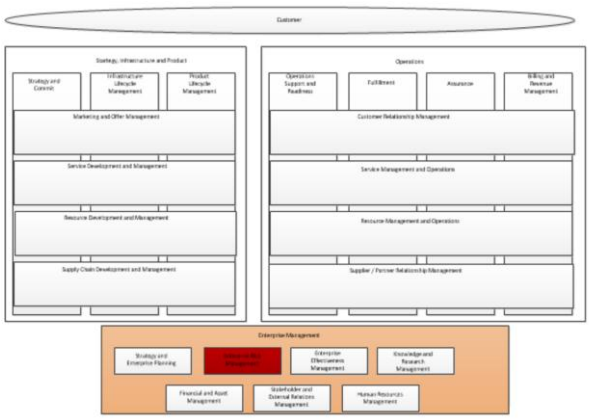

Figure 4-13: Enterprise Management - Enterprise Risk Management

SOCs should ensure that they are resilient with respect to business interruptions. This includes bandwidth, facilities as well as IT equipment. SOCs cannot afford to lose data or miss attacks that are in progress. There should therefore be proper, tested business continuity plans in place. Resilience should be built in as part of the design.

- Security Management (1.3.2.2)

  The Security Management process appraises threats to the organisation, and provides controls and capabilities to minimize the threats (TMForum, 2013).

  - Manage Proactive Security Management (1.3.2.2.1)

    The Manage Proactive Security Management process supports the categorization and prioritisation of the threat, and also deals with the enterprise's (SOC's) potential loss of value and damage to reputation (TMForum, 2013).

    SOC service providers should have a risk management strategy in place. SOCs that are compromised by threats have to protect their customers from having to close their doors. The same applies to internal SOCs. The risk management strategy should focus on identifying risks to the SOC, prioritising and measuring the impact, and then mitigating the risk.

  - Define Security Management Prevention (1.3.2.2.8)

    The Define Security Management Prevention process deals with the specification of baseline security controls and operational policies to be deployed in the enterprise. During this process, decisions are made regarding the assets that should be protected, the means that should be used to do so and the assurance levels that would be appropriate (TMForum, 2013).

    SOCs should have a security baseline, which should adhere to legal and governance requirements, as well as to organisational requirements. This includes a risk management strategy, an asset identification and classification scheme and a vulnerability management strategy.

  - Monitor Industry Trends for Security Management (1.3.2.2.2)

    The Monitor Industry Trends for Security Management process addresses the aspect of monitoring industry trends as well as best practice approaches to

ensure that the enterprise stays at the forefront of minimisation of threats to security management (TMForum, 2013).

Over and above the fact that SOCs should do this as part of their own risk- and threat mitigation strategy, this should also be a service that is offered by SOC service providers to their clients, and by internal SOCs to the organisation. This information should be communicated daily, with mitigation and containment procedures as part of the communique.

- Define Monitoring to Facilitate Security Management (1.3.2.2.9)

  The Define Monitoring to Facilitate Security Management process focuses on the collection, filtering, aggregation, distribution and retention of relevant data from managed resources and services (TMForum, 2013).

  SOCs serve as an outsourced monitoring capability for clients, or as an internal capability for the organisation. However, they should also monitor their own resources in order to detect anomalies and breaches, and to respond to them. Aggregation is a bone of contention: for forensic requirements, some organisations may decide not to aggregate events.

- Define Security Management Policies and Procedures (1.3.2.2.3)

  The Define Security Management Policies and Procedures process defines the policies, guidelines, practices and procedures to be followed. It is also responsible for setting Security Management corporate policies, guidelines, best practices and auditing requirements for compliance by the enterprise. Security Management addresses internal and external sources of security violations. Note that Audit Management processes provide the assurance that the necessary control structures are in place, and provide an estimate of the extent to which the procedures are followed and are effective (TMForum, 2013).

  There should be a process in place that defines all policies, processes and procedures that are applicable to SOCs. This will differ between the two entities, since SOCs may have to adhere to the governance requirements of clients, as well as to their own requirements. Internal SOCs are subject to the organisation's demands. These could include policies such as encryption, back-up policies, incident management processes and incident management procedures.

- Define Security Management Analysis (1.3.2.2.10)

  The Define Security Management Analysis process defines the policy-based assessment of collected or correlated data for events or trends of interest (TMForum, 2013).

  SOCs will usually collect events, correlate them and trigger automated workflows. Events should also be kept for a certain period of time as specified by the client or by legal and governance requirements. This allows for trend analysis. This process also implies that a reaction mechanism needs to be in place, should any anomalies or unwanted trends be found. This must be done for the SOC's own monitored assets, and also for the monitored assets of clients.

- Assist with Security Management Deployment (1.3.2.2.4)

The Assist with Security Management Deployment process provides support to the enterprise operational areas with the deployment of appropriate physical infrastructure, procedures and monitoring capabilities (TMForum, 2013).

Depending on whether or not SOCs offer managed services, they will have to assist in the deployment, configuration and management of security technical controls. SOCs should also be guiding their clients with respect to the security controls needed. They should further guide their clients or the organisation with respect to effective process and policy development and deployment.

- Manage Reactive Security Management (1.3.2.2.5)

  The Manage Reactive Security Management focus on the establishment of controls and data collection capabilities to capture the details of operational activity (TMForum, 2013).

  SOCs must have the capability to monitor and capture operational processes. They should also monitor organisation- and client data to assist in combatting fraud.

- Define Incident Management policies and Procedures (1.3.2.2.12)

  The Define Incident Management policies and Procedures process describes Information Technology Service Management –based (ITSM-based) incident management practices. Incident Management will identify the necessary response and recovery actions that may be conducted within Operations or Assurance, or Business Continuity Management processes (TMForum, 2013).

  The whole purpose of SOCs is to react and respond to security incidents. There must be an incident management process to follow when incidents are detected. This implies that events must be classified, an escalation matrix must exist, and the process should contain mitigation and containment advice. In the case of managed services, the SOC will drive and execute the containment and mitigation process.

- Detect Potential Security Threats and Violations (1.3.2.2.6)

  The Detect Potential Security Threats and Violations process manages the analysis of monitored activity to detect potential threats or security violations (TMForum, 2013).

  To perform this, SOCs could use SIEM's with correlation rules to detect anomalies or rely on external threat management feeds to provide guidance in building such rules. This also implies well-trained and experienced staff to do analysis on events. This ties in with the incident classification and incident management processes.

- Investigate Potential Security Threats and Violations (1.3.2.2.7)

  The Investigate Potential Security Threats and Violations process addresses forensic investigations in order to determine whether a potential threat is imminent, whether a security violation has occurred, and to identify the potential or actual perpetrators (TMForum, 2013).

SOCs can provide forensic capabilities as additional services. This allows clients or the organisation to be informed as to whether a threat is real and serious, as well as who the possible perpetrators are. External attacks could be traced back to an IP or Internet Service Provider (depending on what is being monitored), or names, office and telephone numbers internally (depending on what is being monitored).

- ITIL IT Service Continuity Management (1.3.2.7)

  Service Continuity Management is defined within ITIL. This process addresses the overall Business Continuity Management within the enterprise (SOC) in order to ensure that the IT systems and support are available within the business, and to recover and restore the IT service as required and agreed when service interruptions arise (TMForum, 2013).

  This differs from Business Continuity Management in that IT continuity is addressed here.

  SOCs should have IT continuity plans in place to ensure the availability or resilience of their IT systems in the event of catastrophe or failure.

- ITIL Information Security Management (1.3.2.8)

  Information Security Management addresses the safety and integrity of information within the enterprise, and aims to satisfy a Service Level Agreement that has been established with the owners or users of the information, concerning these aspects. Issues involved include the availability of the information, and maintenance of its integrity and confidentiality as required and agreed (TMForum, 2013).

  SOCs must deploy administrative and technical controls to protect the, integrity of their systems from a cybersecurity perspective.

- ITIL Problem Management (1.3.2.9)

  ITIL Problem Management is aimed at finding the root cause of a problem. This is not about quickly fixing something, but about ensuring that the fix is permanent once it is implemented (TMForum, 2013).

  Breaches and attacks will occur. Once the investigation and analysis is completed, the problem management process will commence in order to ensure that controls are deployed that will provide a permanent fix to the problem that is being experienced. This is true for line outages as well as for general failures of IT equipment, which affects the availability of the service to clients.

Enterprise Effectiveness Management (1.3.3)

The Enterprise Effectiveness Management position in the eTOM framework is contextualised in Figure 4-14.

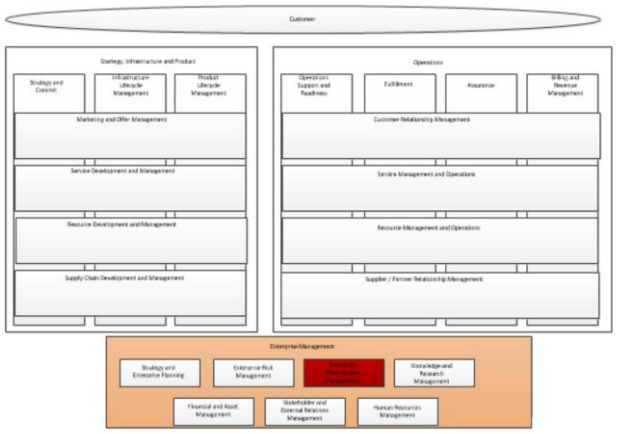

Figure 4-14: Enterprise Management - Enterprise Effectiveness Management

- ITIL Incident Management (1.3.3.9)

  This process manages unplanned interruptions to IT Services, or a reduction in the quality of an IT Service. Failure of configuration items that has not yet impacted services is also seen as an incident (TMForum, 2013).

  SOCs manage IT Security incidents. This is one of their core functions. A properly defined incident management process and procedures must be in place to manage security events that resemble the ITIL incident description.

- ITIL Service Level Management (1.3.3.10)

  The Service Level Managers are responsible for keeping up to date with the current and future service requirements of customers. They also ensure that Service Level Agreements (SLAs) and Service Level Reports (SLRs) are kept up to date and are a true reflection of the business requirements. This process also looks at complaints, audits and customer satisfaction (TMForum, 2013).

  SOCs can choose to sell and manage their services to customers using an SLA approach. These SLAs and other service requirements need to be managed. This is typically true where a client makes use of a managed services offering. SOCs can manage their internal agreements using OLAs. These SLAs and OLAs need to be measureable.

- ITIL Capacity Management (1.3.3.11)

  The Capacity Manager will ensure that there is adequate capacity to meet current and future business needs. This means ensuring that the forecasting of the future need is in place along with measurement of the current usage. This role will ensure that optimization takes place, while at the same time looking forward to what the newly available technology is and will be. Recommendations will be made in line with these findings (TMForum, 2013).

  SOCs must ensure that proper capacity planning is done, specifically when it comes to storage and retention of data, and the processing of events – due to the volume of data that will need to be processed and managed. We would recommend that a surplus

storage capacity of at least 40% should be budgeted for. Other metrics such as CPU and RAM usage must also be monitored, as well as staffing resources and facilities.

- ITIL Availability Management (1.3.3.12)

  The responsibility of the Availability Manager is to effect the achievement of availability targets of current services. The Availability Manager also needs to ensure that newly designed services are delivering on the availability requirements as specified by business. The Availability Manager will help to specify what the reliability, maintainability and serviceability of a new service should be (TMForum, 2013).

  SOCs must have a plan in place to ensure not only IT continuity, but also business and service continuity. This would typically be the Business Continuity Plan (BCP). This includes the classification of services, as well as their criticality and their availability levels.

- ITIL Event Management (1.3.3.7)

  The purpose of event management is the detection of, and response to IT infrastructure events. An event is defined as a detectable and distinguishable occurrence that is important to IT infrastructure managers, and the delivery of IT services. An event is also used to describe the impact that an irregularity might have on a service. Examples of events are notifications created by an IT service, a Configuration Item (CI) or monitoring tools. Not all events need to be actioned or responded to. Responses could range from manual responses, but responses can also be automated. The difference between events and monitoring is that monitoring provides information on everything, and events provide specific and meaningful information and notifications. (TMForum, 2013).

  SOCs should monitor their IT infrastructure for any events that might have an impact on the delivery of service. There must be a process in place that governs the response to events, which might have an impact on service delivery.

Knowledge and Research Management (1.3.4)

The Knowledge and Research Management position in the eTOM framework is contextualised in Figure 4-15.

- Knowledge Management (1.3.4.1)

  The Knowledge Management process is responsible for managing the implied and implicit knowledge within the Enterprise (SOC). Its aim is to facilitate processes and capabilities to ensure that all employees are armed with the knowledge available to enable them to perform their jobs in an effective and efficient manner. It further facilitates the capturing of knowledge generated by work activities, ensures that it is retained, and made available across the organisation. (TMForum, 2013).

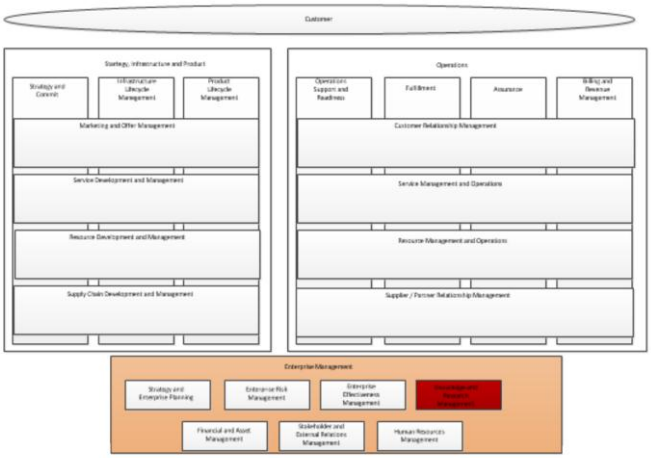

Figure 4-15: Enterprise Management - Knowledge and Research Management

SOCs should have a way of communicating knowledge, processes, procedures, SLAs, knowledge of client infrastructure and threats, shift rosters, etc. so that all staff within the SOC are aware of where to find the knowledge. This has to be updated constantly at pre-defined periods or when any of the aspects or client aspects change.

Any vulnerabilities or threats seen against monitored items should be captured, together with mitigation and containment procedures. This information should be easily accessible, preferably via an internal portal.

- Technology Scanning (1.3.4.3)

  The Technology Scanning process describes the research and initial assessment of surfacing technologies from vendors and other external sources. The process describes the identification and evaluation of technologies and sources, and their comparison with in-house research capabilities. The business value of emerging technology procurement, as well as commitments in terms of the actual acquisition of technologies is also described (TMForum, 2013).

  SOC service providers must constantly scan the market for new and emerging technologies. This would allow them access to additional revenue streams, better protection for customers, better advice to customers and give them a competitive edge over the competition.

  Internal SOCs should do the same so as to allow them to better protect and guide the organisation that they serve by leveraging new capabilities.

Financial and Asset Management (1.3.5)

The Financial and Asset Management position in the eTOM framework is contextualised in Figure 4-16.

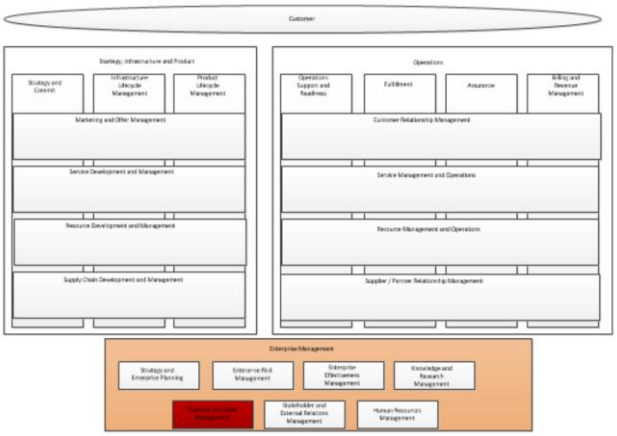

Figure 4-16: Enterprise Management - Financial and Asset Management

- Financial Management (1.3.5.1)

  Financial Management processes manage the financial aspects of organisations like Treasury, Banking, Payroll, Financial Planning, as well as Accounting Operations functions such as Accounts Receivable and Payable (TMForum, 2013).

  SOC service providers should have a financial management process in place. This will allow for timely and accurate billing of clients, paying rent, technology licences and maintenance as well as salaries and wages.

  Internal SOCs should do the same, depending on whether or not they are run as a separate cost center.

- Asset Management (1.3.5.2)

  The financial and policy components of an organisation's physical assets are described by the Asset Management process. This includes elements such as moveable assets, infrastructure and stocks. The process describes asset management policies, the tracking of assets using asset recording systems and the management of the organisational asset balance sheet. (TMForum, 2013).

  All SOCs must have an asset management process in place. This ensures that assets are properly managed. Assets include people, technology, intellectual property and information. This process will also assign a classification scheme to assets, and will collaborate closely with the security process to ensure that assets are properly protected by means of administrative and technical controls.

Stakeholder and External Relations Management (1.3.6)

The Stakeholder and External Relations position in the eTOM framework is contextualised in Figure 4-17.

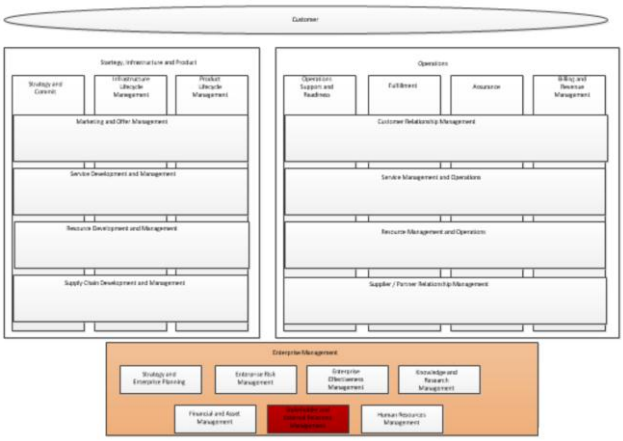

Figure 4-17: Enterprise Management - Stakeholder and External Relations Management

- Corporate Communications and Image Management (1.3.6.1)

  Corporate Communications and Image Management processes are responsible for conveying the appropriate messages to the market and industry about the holistic business (SOC). These processes includes the promotion of the desired corporate image for the organisation as well as the promotion of its general business and products. (TMForum, 2013).

  SOCs need to have a marketing plan and strategy for selling and promoting their services to clients and prospective clients. Internal communication is also important to keep staff informed about new developments, marketing campaigns and service offerings.

  SOCs communication will be internally focused, informing management and sponsors about services and capabilities, as well as of achievements and the value that its services add to the organisation.

- Regulatory Management (1.3.6.4)

  Regulatory Management processes ensure that the organisation identifies all applicable government and legal requirements, and complies with them. (TMForum, 2013).

  This is an important aspect from a SOC service provider perspective. Not only do SOCs have to comply with their own internal and country-specific legal and governance requirements, but they should keep in mind customers' requirements from different sectors such as finance and government. If they provide a global service, the country-specific legal and other requirements also need to be kept in mind.

  SOCs will need to comply with internal requirements, but should also take cognisance of the requirements of other countries, should they have a global presence.

Human Resources Management (1.3.7)

The Human Resource Management position in the eTOM framework is contextualised in Figure 4-18.

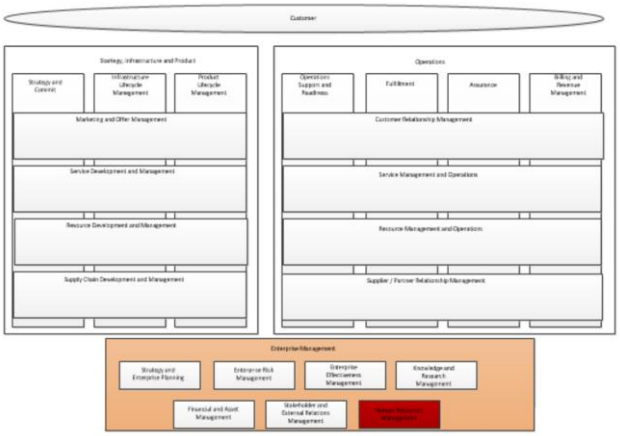

Figure 4-18: Enterprise Management - Human Resources Management

- HR Policies and Practices (1.3.7.1)

  The HR Policies and Practices process describes the processes in support of the management of human resources. The process describes aspects such as performance management, remuneration policies and levels, allowances and benefits and equal employment policy. Mechanisms to measure and manage the performance and satisfaction levels of employees are also described. (TMForum, 2013).

  - Facilitate Performance Appraisal (1.3.7.1.1)

    This is an important process in the management of staff. Staff should firstly be aware of what they are supposed to do by means of Key Performance Indicators (KPIs) or job descriptions. This needs to be measureable. Staff should also be given feedback on how they are performing, as well as on areas in which they could improve. This process includes aspects such as career planning and course planning.

  - Facilitate Remuneration Policies and Levels (1.3.7.1.1)

    SOCs will typically have staff with different skills and experience levels. Remuneration should be adjusted accordingly, so that staff with higher qualifications and experience is typically paid more (although this is not always the case). Also, staff will have something to aspire to as they climb the career ladder within the SOC. A typical SOC operation will have Level 1 Engineers responsible for monitoring, analysis and incident management and escalation, Level 2 Engineers responsible to support technical controls, and Level 3 Engineers responsible for Security Architecture design. The SOC Manager and SOC Supervisor are included as management overheads.

  - Facilitate Allowances and Benefits (1.3.1.7.2)

    In some instances it may be necessary for staff to work overtime (such as in the case of a malware outbreak and the ensuing mitigation and containment effort). It may also be necessary to provide on-site or telephone support in cases where clients are requesting such services. In these cases, the aspects that should be addressed include, but are not limited to (TMForum, 2013):

    - Travel allowances
    - Fuel and toll allowance
    - Cell phone allowance

- Overtime
- Sustenance and Travel allowance

- Facilitate Occupational Health and Safety (1.3.7.1.3)

  All occupational health and safety acts should be adhered to.

- Facilitate Code of Conduct (1.3.7.1.6)

  This would be captured in the HR policy. SOCs will have their own code of conduct, but in some cases SOCs will adhere to the organisation's code of conduct. This includes aspects such as dress code, substance abuse, etc.

- Facilitate Hiring and Termination Guidelines (1.3.7.1.7)

  This process addresses the hiring of staff as well as the termination of employments. This addresses, but is not limited to, aspects such as background checks, qualification checks and exit interviews (TMForum, 2013).

- Facilitate Employee Satisfaction measurement and Management

  Satisfied and happy employees are more productive and add more value to the organisation. Employee satisfaction and morale should be managed and measured in order to determine causes for unhappiness and to address these as soon as possible.

- Workforce Development (1.3.7.4)

  Workforce Development processes focus on development of employees to meet the needs of the business. These processes include competency modelling, skills assessment, job and employee strength profiling, succession planning, training development and delivery, career development, work design, employee recruitment, etc (TMForum, 2013).

  Succession planning is an integral part of managing a successful SOC. This could be achieved by cross-training and on-the-job training. Staff should also be evaluated on their strong and weak points, and should be deployed accordingly. Furthermore, staff should attend the correct course or training that is either facilitated in-house or by external providers.

Figures 4-19 to 4-21 highlight the areas that are mapped back to SOC requirements.
Appendix D is a complete, consolidated framework that includes ITIL, ISO/IEC 27001:2005 and CoBIT aspects.

Figure 4-18 is a visual representation of the Strategy, Infrastructure and Product section of the eTOM framework mapped back to SOC requirements. The SOC requirements are consolidated here. Figure 4-19 consolidates all SOC requirements from an Operations perspective, and Figure 4-20 consolidates Enterprise Management aspects. The smaller figures at the top indicate the position inside the eTOM framework.

4.5 Summary

In the preceding chapters, all SOC requirements were identified and the rationale behind the inclusion of requirements was supplied. A comprehensive set of requirements has now been defined, and is supported by industry-accepted standards and frameworks. In some cases such as operations, ITIL would be a better fit than eTOM. Furthermore, SO/IEC 27002:2005 would be a better fit from a risk management perspective. eTOM provides better coverage when looking at business requirements. This is illustrated in Table 3-11 in Chapter 3.

The SOC consolidated framework is attached in Appendix D.

Now that the SOC requirements have been determined, a method for measuring the maturity and effectiveness of the functions needs to be developed. This will be addressed in Chapter 5.

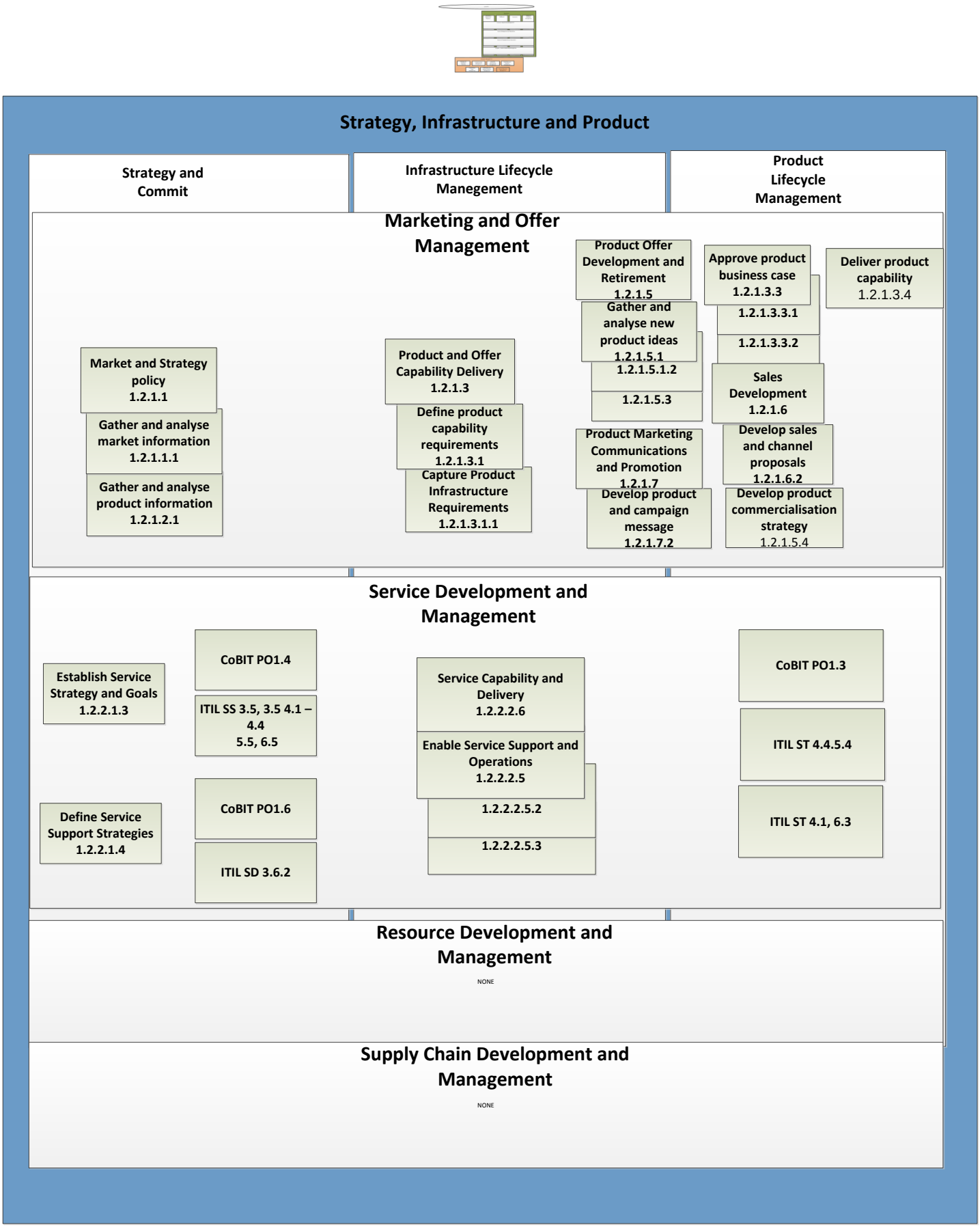

Figure 4-19: SOC Framework: Strategy, Infrastrucure and Product

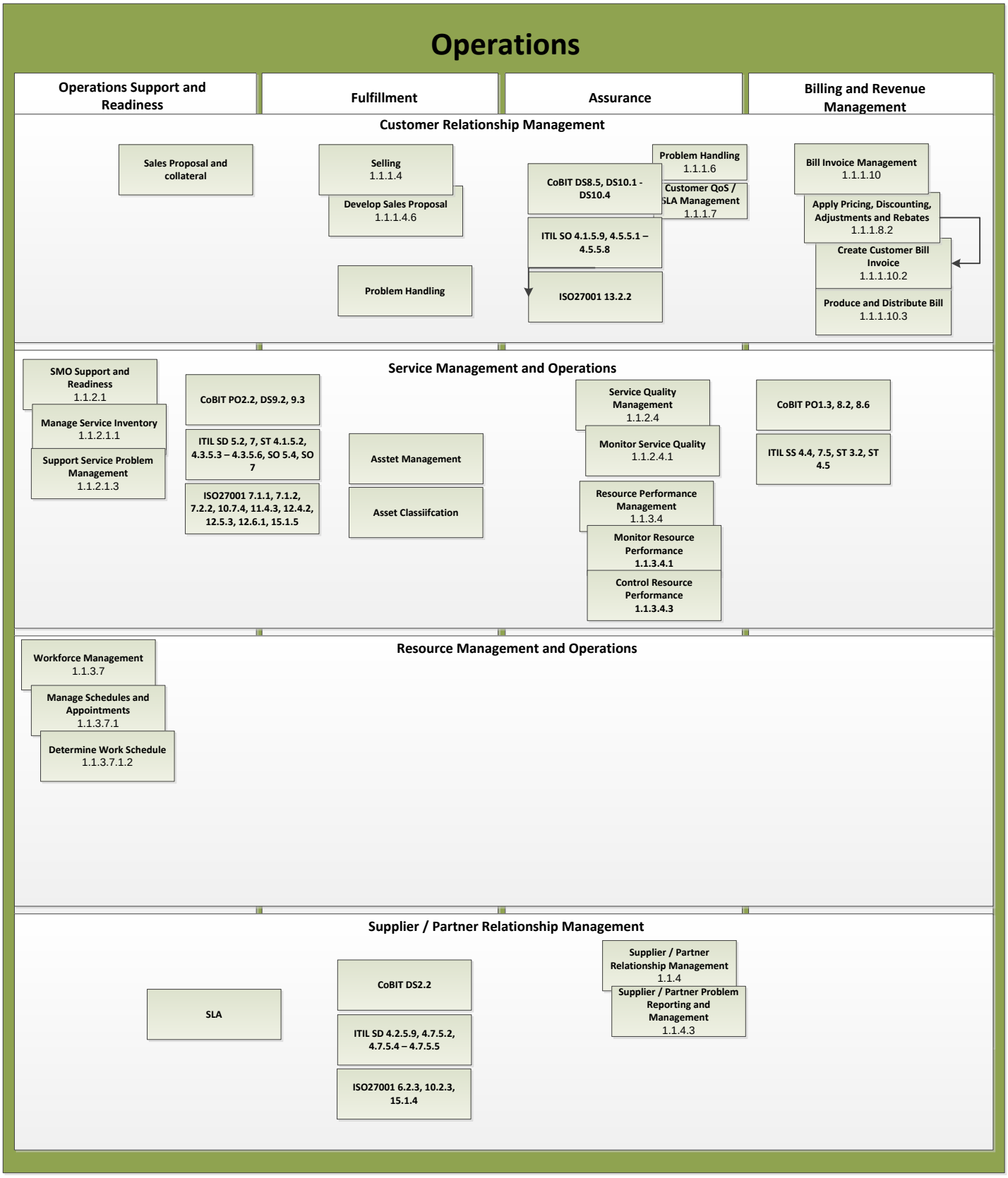

Figure 4-20: SOC Framework: Operations

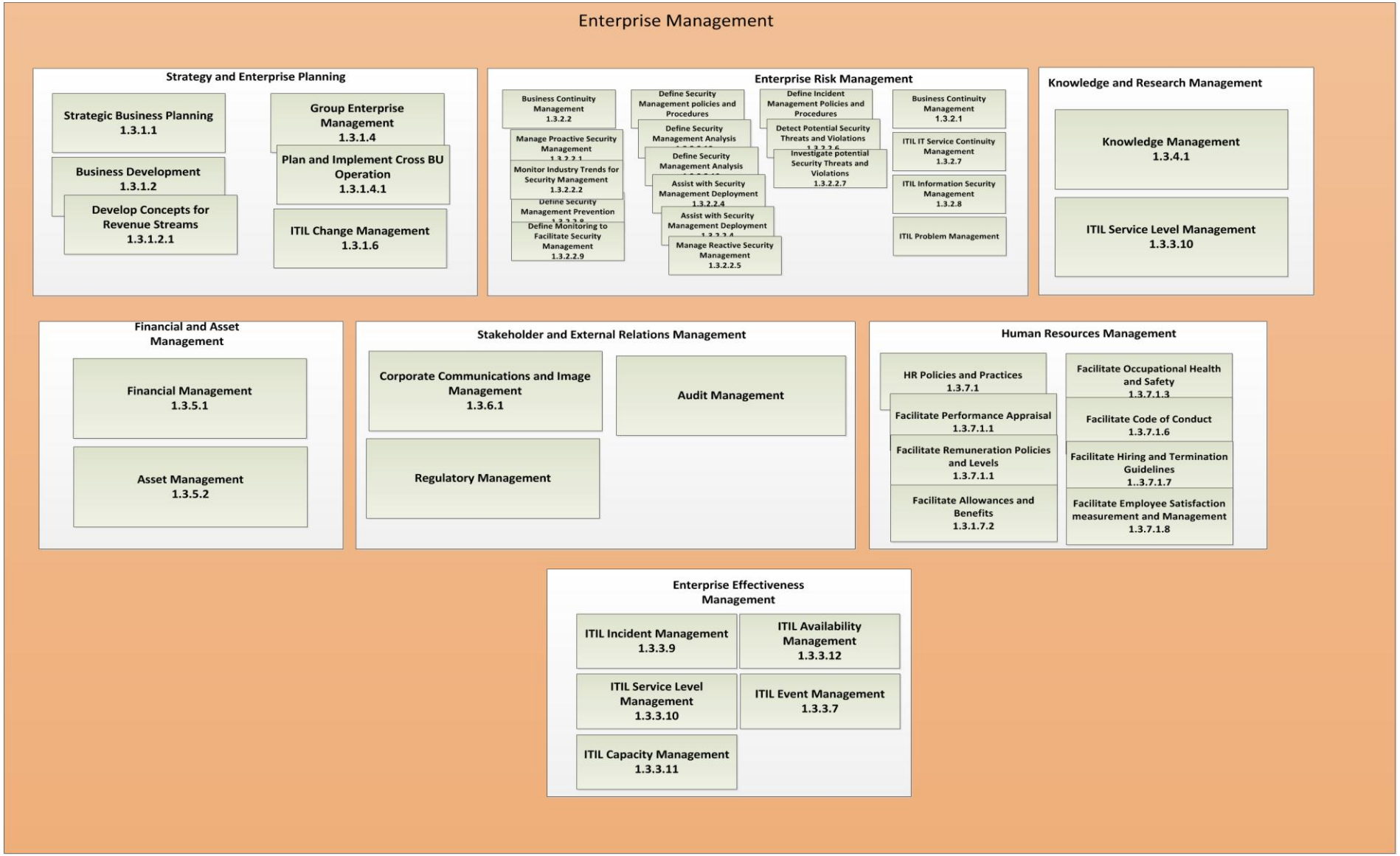

Figure 4-21: SOC Framework: Enterprise Management

5 SOC Maturity and Effectiveness Measurement

5.1 Introduction

With the SOC framework developed, and functional requirements determined, there needs to be a mechanism to measure the effectiveness of the functional requirements, and the maturity of the SOC as a whole.

The purpose of this chapter is to propose a SOC measurement and classification scheme that can be used by vendors and service providers alike to score the service offering, as well as to give service providers the opportunity to improve where necessary.

As already mentioned, there are numerous frameworks for technologies that are used in SOCs (Bidou, 2004; Kelley *et al.,* 2006; Madani *et al.,* 2011). However, there is no holistic framework addressing processes, staffing and technology aspects of a SOC. There are also developed methodologies for benchmarking technologies used in SOCs such as SIEM and its capabilities (Butler, 2009). In our research, we could not find any model that could be used to classify SOCs. We will therefore base the classification model on industry-accepted models.

We present a model to measure the effectiveness and capabilities of a SOC, through three aspects:

- The functional requirements of SOC services;
- The measures of effectiveness of functional requirements; and
- The Maturity of SOC functional requirements.

Maturity models or frameworks implies perfect or explicitly defined, managed, measured and controlled systems (Pederiva, 2003; Al-Mayahi & Mansoor, 2012). A Maturity framework will be coupled with capabilities to create a classification matrix. With this classification matrix, we will try to provide consumers of SOC services with a reference when building their own SOCs, or when choosing a vendor that will be providing those services. We do not aim to define the exhaustive list of functional aspects of a SOC, but rather to define the critical aspects as per the proposed framework, and this model can be expanded upon with further functional aspects.

In this Chapter, a maturity score is developed for SOCs using a combination of existing maturity models. A Mechanism to measure the effectiveness of a SOCs capabilities is then developed and proposed. This is called the SOC classification cube, and includes the number of capabilities, their effectiveness and maturity to derive a score out of 100.

5.2 Industry-accepted maturity models

When describing the maturity level of a SOC, it would be prudent to use existing established IT management frameworks such as CoBIT and ITIL (OGC, 2000; Adler, 2007), coupled with information security frameworks such as ISO 27001. The CoBIT framework covers aspects of IT in the business, and is supported by ITIL, which covers effectiveness and efficiency of operations.

In order to have a repeatable model, SOCs will have to be classified for each functional requirement, the MoE's (how effective functional requirements are offered), and the maturity (how well the SOC can deliver the functionality).

CoBIT identifies five maturity levels for the management and control of IT processes, which allows for benchmarking and identification of capability improvements (Adler, 2007). This approach was derived from the Software Engineering Institute (SEI) (Adler, 2007a).

The five CoBIT maturity levels as per Adler, (2007) are:

- 0 Non-existent
- 1 Initial/Ad Hoc
- 2 Repeatable but Intuitive
- 3 Defined Process
- 4 Managed and Measureable
- 5 Optimized

These maturity levels are not absolutes and it is not something that can be measured with 100% accuracy, since some implementations will be in place at different levels. However, these levels will assist in creating a profile of the current level of maturity.

The ITIL Process Maturity Framework (PMF) also identifies five Process Maturity Levels (MacDonald, 2010). As illustrated in Figure 2-10, ITIL focuses more on the Operational aspects of the IT Key concepts, and this is reflected in the fact that their framework addresses Process Maturity.

The five ITIL Process Maturity Framework maturity levels as described by MacDonald, (2010) are:

- 1 Initial
- 2 Repeatable
- 3 Defined
- 4 Managed
- 5 Optimised

ITIL was used to determine the SOC requirements when looking at the eTOM Enterprise Management section of the eTOM framework as indicated in Chapter 3 and 4. In addition, it was also identified as the preferred framework to support SOC Operational aspects as indicated in Chapter 2, such as change management, incident management and problem management.

According to Wim Van Grembergen and Des Haes (2005), "The control objectives of COBIT indicate for the different IT processes what has to be accomplished, whereas other standards, such as ITIL, describe in detail how specific IT processes can be organised and managed". It needs to be noted that none of these maturity models addresses risk as part of their levels.

The Software Capability Maturity Model (CMM) also recognizes five maturity levels The Capability Maturity Model (CMM) focuses on organisations' software processes, and the evaluation of the capability of these processes (Curtis *et al,* 1993) and (ITGovernanceUSA, 2011). The CMM Model is depicted in Figure 5-1.

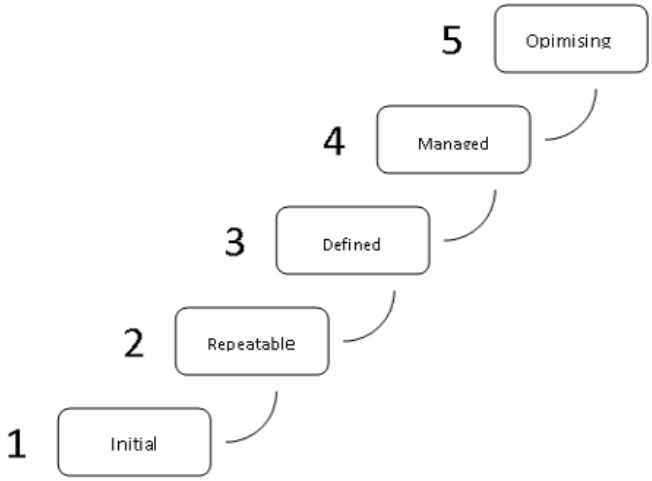

Figure 5-1: CMM Maturity Model (ITGovernanceUSA, 2011)

The National Institute of Standards and Technology (NIST, 2012) uses five security maturity levels defined as:

- IT Security Maturity Level 1: Policies;
- IT Security Maturity Level 2: Procedures;
- IT Security Maturity Level 3: Implementation;
- IT Security Maturity Level 4: Test; and
- IT Security Maturity Level 5: Integration.

The International Systems Security Engineering Association (ISSEA) has developed a Capability Maturity Model (CMM). This is called the Systems Security Engineering Capability Maturity Model (SSE-CMM) (Phillips, 2003). The five capability levels as reproduced from Phillips (2003) are:

- Level 1 – Base practices are performed informally;
- Level 2 – Base practices are planned and tracked;
- Level 3 – Base practices are well defined;
- Level 4 – Base practices are quantitatively controlled; and
- Level 5 – Base practices are continuously improving.

A systematic approach to measuring the maturity of a security technical or administrative control should (Phillips, 2003):

- Generate reproducible and justifiable measurements of the security posture and service to organisation or client;
- Measure something of value to the client or organisation;
- Determine progress in security posture and service delivery to clients; and
- Assist in determining the order in which security controls should be applied as well as the resources needed to apply the security program.

The CERT/CSO Security Capability Assessment model consist of five maturity levels (Sajko, 2007). These are aimed at the quality of documentation. The levels as defined by Sajko (2007) are:

- Level 1 – Exists
- Level 2 – Repeatable

- Level 3 – Assigned Responsibility
- Level 4 – Documented
- Level 5 – Revised and Updated

Table 5-1 summarizes the published Security Maturity Models and their focus as reproduced from Akridge & Chapin (2005) The derived proposed SOC Process Maturity model is summarised in Table 5-1.

Table 5-1: Published Security Models and their Focus (Akridge *et al.,* 2005)

Model	Description	Comments
NIST CSEAT IT Security Maturity Model	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)	Five levels of progressive maturity: 1. Complacency 2. Acknowledgment 3. Integration 4. Common practice 5. Continuous improvement	Focused toward organisational awareness and adoption
COBIT® Maturity Model	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	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	Five levels of progressive maturity: 1. Exists 2. Repeatable 3. Designated person 4. Documented 5. Reviewed and updated Measured using four levels: 1. Initial 2. Evolving 3. Established 4. Managed	Focused toward measurement of quality relative to levels of documentation

5.1 SOC maturity model

The six-step model that is proposed, is consistent with all the published Security Maturity Models, and can be cross-referenced to a more than one model per specific maturity level.

Table 5-2: SOC Maturity Model

Level	Name	Alignment
0	**Non-existent**	CoBIT 0, etc.
1	**Initial**	CoBIT, SSE, ITIL: Initial CERT: Exists
2	**Repeatable**	(CoBIT, ITIL, SSE-CMM and CERT/CSO)
3	**Defined Process**	(CERT/CSO)/Well Defined (SSE-CMM), Defined Process (CoBIT), Common Practice (CITI-ISEM)
4	**Reviewed and updated**	(CERT/CSO), Quantitatively controlled (SSE-CMM), Managed and Measureable (CoBIT) and Continuous Improvement (CITI-ISEM)
5	**Continuously Optimised**	Optimised (CoBIT), Continuously Improving (CITI-(ISEM), Continuously Improving (SSE-CMM)

HP uses a similar model, as reproduced in Table 5-3, when assessing the maturity of their client's SOCs which aligns with the proposed maturity model (Hewlett-Packard, 2012).

Table 5-3: HP SOC Maturity Model (Hewlett-Packard, 2012)

SOMM Level	Name	Description
Level 0	Incomplete	Operational elements do not exist
Level 1	Performed	Minimum compliance requirements to provide security monitoring are met
Level 2	Managed	Business goals are met and operational tasks are repeatable
Level 3	Defined	Well-defined, subjectively evaluated and flexible operations
Level 4	Measured	Operations are quantitatively evaluated, consistently reviewed and proactively improved
Level 5	Optimizing	Operational improvement program has been implemented to track any deficiencies and ensure that all lessons learnt continually drive improvement

5.2 Framework Requirement Measures of Effectiveness (MoE's)

SOC requirements are numerous, and should constantly be updated. Functional requirements describe the functionalities of a SOC, and (MoE's) describe how well it performs these functions (Warda, 2005; Reply Communication Valley, 2011).

In order to be able to compare different SOCs, it is important to have defined functional requirements against which they can be measured. These can be grouped into Strategy, Infrastructure and Product, Operations and Enterprise as per the proposed framework. The functional requirements can be expanded with MoE's that can be measured on their maturity.

In chapter 5, we have identified the SOC requirements based on functional requirements, service requirements and business requirements, with people requirements part of the business requirements.

SOC requirements were identified by defining the functional capabilities that a SOC should have, as well as a combination of a number of security management and control frameworks (Protz, 2005; Cisco Systems, 2006; Kelley *et al.*, 2006; Del Vecchio, 2012), including ISO 27000 series and SANS Critical Controls (Warda, 2005).

The business requirements are listed in Table 5-4 as reproduced from TMForum (2013). The requirements will have detailed MoE's listed under them. The requirements will be scored from 0 to a maximum of 5. If a requirement exists, it can either be marginally capable, or it can have a high capability. The capabilities are rated from 0 – 5 with 0 a function having a non-existent capability, and 5 a function with a high capability. This is illustrated with the following example:

In terms of monitoring a SOC will have a capability of 1 if it can monitor from a limited number of vendors, a limited number of devices, such as the limited capability of being able to monitor only 3 firewalls, intrusion prevention systems and mail content filters from 2 vendors, Cisco and CheckPoint. A SOC with a high capability of 5 will be able to monitor multiple devices from most vendors

Table 5-4: SOC business functions (TMForum, 2013)

Strategy, Infrastructure and Product (Component)	**Operations (Component)**	**Enterprise (Component)**
Aspects		
✓ Market and Strategy Policy ✓ Product and Offer Portfolio Planning ✓ Product and Offer Capability Delivery ✓ Product and Offer Development and Retirement ✓ Sales Development ✓ Product Marketing Communications and Promotion ✓ Service Strategy and Planning ✓ Service Capability Delivery ✓ Customer Relationship Management	✓ Customer Relationship Management ✓ Service Management and Operations ✓ Resource Performance Management ✓ Workforce Management ✓ Supplier/Partner Relationship Management	✓ Strategic and Enterprise Planning ✓ Enterprise Risk Management ✓ Enterprise Effectiveness Management ✓ Financial and Asset Management ✓ Stakeholder and External Relations Management ✓ Human Resources Management

In order to determine the score, the effectiveness of the requirements needs to be measureable. For the purpose of illustrating the concept of how a score is derived, three examples will be used.

5.2.1 MoE First sample

The scoring is done as follows: Capabilities will be listed according to the framework. In the case of Strategy, Infrastructure and Product, and for the purpose of illustrating the scoring mechanism, 2 requirements were identified. A SOC with a low capability will fulfil none, or 1 of the requirements. After the number of capabilities have been identified, their MoE's are scored, as well as the maturity levels of the supporting processes.

Component: Strategy, Infrastructure and Product

Aspect: Service Strategy and Planning

For this aspect, we have identified two requirements. A SOC with low capability will fulfil only one requirement. A SOC with high capability will fulfil both requirements.

Requirement: Establish Service Strategy and Goals

A SOC with low maturity will have no service strategy and goals defined. A SOC with high maturity will have a well-documented, regularly reviewed and measureable strategy and goals.

Requirement: Define Service Support Strategies

A SOC with low maturity will have no principles, policies and performance standards defined. A SOC with a high maturity will have the above clearly defined, documented, reviewed and measured by clients. These could take the form of SLAs and OLAs.

5.2.2 MoE Second sample

Component: Operations

Aspect: Customer Relationship Management

For this aspect, we have identified four requirements. A SOC with low capability will fulfil only one requirement. A SOC with high capability will fulfil all requirements.

Requirement: Bill Invoice Management

A SOC with low maturity will have no information, systems, material and resources available so as to enable completion of the invoice management without delay. A SOC with high maturity will have information, systems, material and resources available so as to enable completion of invoice management.

Requirement: Selling

A SOC with low maturity will have no or limited means by which to administer and manage the operations of sales channels, and will have no capability such as material, systems and resources to support the sales cycle.

A SOC with high maturity will have the above clearly defined, documented, reviewed and measured by clients. These could include proposals, presentations, pre-sales capability pricing information and other documents.

Requirement: Problem Handling

A SOC with low maturity will not have the capability to manage problems reported by customers. There is no way or method to receive reports from customers, and to resolve the problem to the customer's satisfaction.

A SOC with high maturity will have different channels available to clients for the reporting of problems. There are clearly defined and measureable processes in place to resolve problems logged by clients.

Requirement: Customer QoS/SLA Management

A SOC with low maturity have no process or interface to manage customers such as reception and recording of contracts, directing of inquiries to the correct processes, monitor and control status of inquiries and escalate where necessary, and ensure a consistent image.

A SOC with high maturity will have clearly identified processes in place as well as different interfaces to the client. A consistent image and service is presented.

5.2.3 MoE Third sample

Component: Enterprise

Aspect: Enterprise Effectiveness Management

For this aspect, we have identified five requirements. A SOC with low capability will fulfil only one requirement. A SOC with high capability will fulfil all requirements.

Requirement: ITIL Incident Management

A SOC with low maturity will have no process to manage unplanned interruptions to IT Services, or a reduction in the quality of an IT Service. A SOC with high maturity will have repeatable, reviewed and tested processes in place to ensure continual service improvement.

Requirement: ITIL Service Level Management

A SOC with low maturity will have no appointed Service Level Manager or capability to keep up to date with the current and future service requirements of customers A SOC with high maturity will have the above clearly defined, documented, reviewed and measured by clients.

Requirement: ITIL Capacity Management

A SOC with low maturity will not have the capability to ensure that the forecasting of future needs are in place along with measuring the current usage A SOC with a high maturity will have the capability, and processes in place to ensure that capacity requirements are managed well.

Requirement: ITIL Availability Management

A SOC with a low maturity have no process to ensure that the current service is performing to its availability targets as well as to ensure that new services are designed to deliver the availability levels required by the business A SOC with high maturity will have clearly identified processes and procedures in place.

Requirement: ITIL Event Management

A SOC with a low maturity will have no way of detecting IT infrastructure events, as well as no way of determining the appropriate response to them.

A SOC with a high capability will have clearly defined processes in place.

5.3 Integrated classification model

The cube in Figure 5-2 will assist in assigning a weight and level to SOCs. Due to the importance of Process Maturity, we propose a slightly higher weighting for Maturity. Maturity of processes is weighted higher than capability, since the maintenance, execution and repeatability of the capability is more important than the number of capabilities (Chung, 2006). The three parts of the framework, capability, maturity and MoE can be visualised using the classification cube.

The classification cube uses the requirements as captured in the framework, and applies the MoEs and maturity score to it. The maturity score would be in a range from 0 (non-existent) to 5 (mature and optimised), the requirements would be the total amount of requirements a SOC has and the effectiveness would be scored from 1 (low effectiveness) to 5 (high effectiveness). The determination of the effectiveness parameters will form part of future studies. On the "Maturity" side of the cube, the maturity levels as determined in section 5.1 is represented. The SOC requirements are represented on the "Requirements" side of the cube. These are all the requirements and capabilities as identified in the development of the framework in

Chapter 4. The MoE's are represented at the bottom on the "Measures of Effectiveness" side. These will be determined as part of future studies.

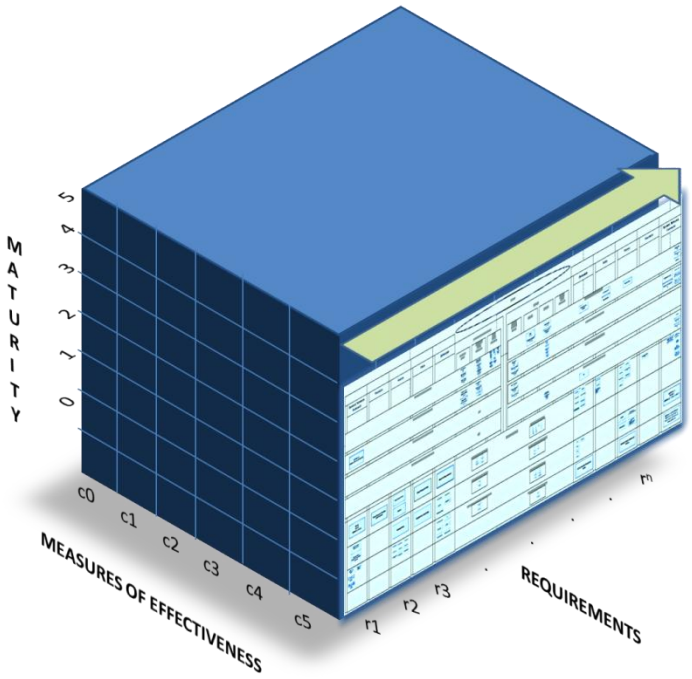

Figure 5-2: SOC Classification Cube

The Maturity, Measures of Effectiveness (MoE's) and Capability of SOCs can be mathematically expressed as follows:

$$S = \frac{\sum_1^n (\alpha C_i + \beta M_i)}{0.05 \times n}$$

Where SOC Score = Sum of all applicable requirements scores, and where each requirement is scored on MoE's and Maturity, expressed as a score out of 100.

α = 0.4 – A lower weight is assigned to capabilities. Capabilities have to be effective in order for them to perform well. The existence of the amount of capabilities is of lesser importance than the MoE's assigned to them.

ß = 0.6 – A higher weighting is assigned to maturity. A Capability could exist, but if the maturity of the supporting processes is not high, then the capability will perform poorly, or not at all.

0.05 – This variable ensures that the score will be out of 100 regardless of the amount of capabilities, its effectiveness and maturity.

The maturity of a requirement weighs more than the effectiveness of a requirement. One could have a requirement but if the maturity is low, the service will not be executed properly.

To balance the scoring, and to indicate the higher importance of maturity over effectiveness, a α value of 0.4 were chosen for the effectiveness of the requirement, which would give the effectiveness score a lesser impact than the maturity requirement score, which is scored higher with ß at 0.6.

This will provide a weighting that can be referenced against the provided map. SOC Managers and customers should strive for a high maturity and high capability level. Based on the business requirements, it would also be possible to weigh specific requirements higher than

others. This could be based on the difference in requirements such as log storage requirements between a financial institution and a school.

This will give consumers of SOC services a classification scheme and reference framework from which to work when choosing a partner or building an in-house solution.

5.4 Summary

The proposed classification system, by making use of framework components mapped to aspects and requirements, provides a model for scoring SOCs so as to allow prospective consumers to make an informed decision. It also allows existing service providers to test their offering, and to improve where necessary.

A SOC maturity scale was determined, ranging from 0 (non-existent) to 5 (mature and optimised. This is then added to the number of requirements a SOC meets, and their MoE's measured from 1 (low) to 5 (high).This allows for the calculation of a score to reflect the effectiveness and maturity of SOCs. The SOC Functional Requirements and Scoring Sheet are attached as Appendix E.

In Chapter 6 we will validate the SOC framework using expert reviewers, and also conduct an assessment of South African and Korean SOC service providers.

6 Framework Validation

6.1 Introduction

Due to the lack of existing frameworks against which to measure, we have decided to test the framework against the experience of industry experts. The completed framework and classification scheme was taken to industry, and a validation process was started. To assist with the validation and verification, a presentation was developed explaining the process and methodology followed in the development of the framework. A Spreadsheet was developed containing the functional requirements, service requirements and business requirements, their MoE's and maturity, bound together by a formula calculating the scores provided during structured interviews. The spreadsheet is attached as Appendix F:

This spreadsheet was the introduced to the expert reviewers, after the presentation, and they were asked to comment on the applicability of the functional, service, business requirements and service requirements. Only two expert reviewers were identified as having sufficient experience in building SOCs, as well as have a thorough understanding of service, business and security concepts. The exact same approach was followed during the assessment of the South African SOC service providers.

A total of four South African SOC Service (MSSP) providers and one Korean SOC service provider were interviewed. Four experts were approached of which two experts were interviewed to obtain their opinion on the framework. This information was obtained during structured interviews with the experts as well as with SOC and MSSP service providers. The problem statement, methodology and outcomes were presented to experts as well as to SOC and MSSP providers. The functional requirements and measures of effectiveness were then presented to them, after which they were given a chance to comment on the content. The SOC reviews were done using the same method. Two expert reviewers gave their input. Four South African SOC and MSSP providers were rated, and their input received on the framework.

The companies and management level who participated in the review process are listed in Table 6-1:

Table 6-1: Companies Interviewed

Company	Person Interviewed
GSOC – South Africa	SOC Manager
Datacentrix – South Africa	SOC Technical Manager
Altech Card Solutions (ACS) – South Africa	SOC Service Delivery Manager
T-Systems South Africa	SOC Manager
IglooSec – South Korea	SOC Manager

In all instances, the South African SOC providers have rated themselves extremely high. It is the opinion of the author that none of these SOC providers actually measure up to the ratings that they gave themselves.

It was also difficult to measure and substantiate the South African SOC's claims without some form of auditing or inspection. This is further exacerbated by the fact that the Korean SOC was visually inspected, demonstrations given and documented proof supplied in support of claims made against the framework. The Korean SOC was used as a baseline against which the South African SOCs were measured since they can be classified as a 5th Generation SOC having met all the requirements of a 5th Generation SOC.

Other factors to consider when considering their claims are:

- None of the South African SOCs have a track record of being involved in any major security related incidents,
- Marketing material on their websites do not measure up against the sales and marketing criteria as expressed in the framework,
- The HR processes do not seem to measure up against the requirements of the framework.
- Some requirements are met from a purely technological perspective such as reports in different formats, delivered via different platforms, analysis and schedules, but these are not presented to their clients as a service. This means the capability is there from a technology perspective, but the maturity of the service to the clients is low or non-existent.

For these reasons, their results have not been included in the thesis.

For this review process to be valuable, it has to be performed independently. A process must be followed where documented proof is supplied in terms of ratings submitted by the providers that were interviewed, or visual inspections must be allowed.

It is furthermore the opinion of the author that the Korean SOC scoring is an accurate reflection, since documented proof was supplied, and an inspection was allowed during the interview.

All MSSPs interviewed have expressed the opinion that the framework seems useful, and is complete.

6.2 Completeness

The framework was considered as complete by both expert reviewers. Their remarks are included in section 6.2.1 and 6.2.2.

6.2.1 Expert Reviewer # 1 Dr Andrew Hutchison

Dr Hutchison works at T-Systems as lead of the global Security Offering team. In addition to numerous management positions within T-Systems (in South Africa, as well as in the global organisation), he has been instrumental in defining the security offerings for T-Systems, including SOC services. Dr Hutchison is an Adjunct Professor at the University of Cape Town, and has also been a participant in the MASSIF project, which investigates solutions for next-generation SIEM technologies. Thus, we believe that he has the experience and expertise to review the proposed solution.

6.2.2 Summary

It is very useful to have a framework, and the framework seems useful. The framework is complete, but should be grouped to mimic the ITIL “Plan, Build and Run” aspects. The framework should also cater for the requirements of next-generation SOCs. It is further crucial to determine, and align the framework with, business requirements.

6.2.3 Expert Reviewer # 2 Marco Perreira

Mr Perreira works at Hewlett Packard as part of the Security Sales team. Previously, he was the EMEA Security Practice Manager for WIPRO where he was responsible for developing and delivering security offerings, including SOC services across multiple WIPRO clients. Thus, we believe that he has the experience and expertise to review the proposed solution.

6.2.4 Summary

eTOM is a good fit if companies are using the entire SOC value chain. The framework is not as applicable to internal SOCs as it is to MSSP's, since internal SOCs will conform to the organisation's business processes. It is very important to map business processes to SOC functions, and these business processes need to be mapped back to the framework. Next-generation SOC requirements should be included and catered for in the framework.

6.3 Chapter Summary

In conclusion it can be said that both expert reviewers agree that the framework is useful and complete. There should be a focus on business requirements, which could be addressed with a architecture philosophy such as TOGAF.

The framework should also be future-proof, and the ability to use the framework for next-generation SOCs must exist. This is fulfilled in the sense that aspects relating to next-generation SOCs such as security awareness training and device management are included. The framework mapping back to business requirements could be improved on.

Gaps still exist with respect to the completeness of the MoE's, but these would be addressed in future studies.

The detailed comments are contained in Appendix F.

7 Conclusion

7.1 Introduction

In this chapter, the conclusions and recommendations following the completion of the study are made.

More and more organisations are building their own SOCs, or become consumers of SOC services due to the proliferation in cybercrime activities, as well as a heightened awareness of the importance of cyber security and the management thereof.

Also, as part of a good all round security strategy, and as mandated by various standards, frameworks and best practices, it is important that security controls as well as other critical assets are monitored to assist in the prevention and detection of attacks.

This study has shown that there is currently no framework for the building and management of SOCs.

A framework was proposed based on industry accepted standards, and frameworks. The framework was determined by deconstructing SOC requirements using Systems Engineering principles. In addition, a SOC classification guide was also developed using the framework, and assigning MoE's to the requirements.

Since there are no existing SOC frameworks covering functional, service and business requirements, no means existed to validate the framework against an existing framework. To compensate for this, reviews were conducted with two experts in the field, and the validity of the framework was also tested against the feedback from existing SOCs, MSSPs and their managers.

7.2 Summary of work

Chapter 1 served as an introduction into what a SOC is, what it does, as well as the drivers behind building or utilising SOC services. The problem was also stated, and the following problems needed to be addressed:

- That there is not a comprehensive SOC framework to be used when designing, building and managing SOCs
- No mechanism or model for measuring the effectiveness of SOCs exists
- No mechanism or model for measuring the maturity of SOCs exists

The objectives of the study were also stated, which was to create a SOC framework, as well as a mechanism to measure the effectiveness of SOCs. Research tasks were deconstructed and listed. These are:

- Development of SOC functional, business and service requirements in Section **Error! eference source not found.**.
- Develop the requirements MoE's in Section 5.2.
- Develop the framework in Chapter 4.
- Develop a classification mechanism in Section 5.3.

All the above would be achieved using Systems Engineering principles.

Chapter 2 consisted of the literature survey. The fact that no existing SOC framework could be found during research was highlighted.

An introduction was made to the framework and standards identified for the development of the framework, as well as the rationale for their selection was made. These are:

- CoBIT 4.1
- ISO 27001:2005
- ITIL v3
- Telecommunications Management Forum's eTOM framework

Each of their strong and weak points were discussed, as well as their intended fit into the framework. In addition, the principles used in the determination of the framework, Systems Engineering principles were also discussed. Motivation was given for the classification of a SOC as a system, and the framework was developed as if the SOC is a system. The most important factors that need to be highlighted are that the SOC is a system, and its design and development should be aligned with Systems Engineering principles.

In the development of a system, the following has to be determined:

- Functional requirements,
- Service requirements
- Business requirements.
- Determine MoE's for all requirements.

These are determined keeping all internal and external factors having an influence in design in mind.

The chapter concluded with a summary of all standards, frameworks, and Systems Engineering principles, as well as how they all fit together, as well as where and how they will be used in the framework.

In chapter 3, the SOC requirements analysis was conducted. The functional requirements were determined following a holistic approach, inclusive of people, processes and technology. For the purpose of this study, the technology requirement was not included, since the determination of the technical requirements with its MoE's is large enough to serve as a separate study.

The SOC service functions were determined, with the focus on processes. Once the requirements were determined, they were mapped back to ISO/IEC 27001:2005, ITIL v3 and CoBIT 4.1. People requirements were also determined, and these were also mapped back to ISO/IEC 27001:2005, ITIL v3 and CoBIT 4.1.

In chapter 4 the SOC business requirements were determined using the TM Forum's Business Process Framework (eTOM). An overview on how eTOM works is provided, as well as how the business process numbering scheme works. Applicable business processes were identified, as well as a motivation on why they should be included within the SOC framework. At the end of the chapter, the framework is presented per eTOM layer. A Consolidated framework mapping back to eTOM is provided as Appendix D, as part of the chapter.

In chapter 5 a mechanism for determining the maturity as well as the effectiveness of SOCs was developed. The MoE's for all requirements were also determined. This leads to a SOC classification tool which is attached as Appendix E.

Chapter 6 consist of the findings and input of the expert reviewers, as well as input from SOC Managers locally, as well as abroad. All remarks and comments pointed to a complete and useful framework, with suggestions basically mentioning aspects which could be combined, or omitted altogether.

7.3 Review of research goals

In this section, the research goals are reviewed, and a motivation will be supplied as to what degree these goals were achieved.

The first goal was to develop SOC requirements, inclusive of functional, service and business requirements. Business requirements also include all aspects related to people requirements.

This goal was achieved using Systems Engineering principles in Section 2.3. A total of 14 functional requirements were identified in Section **Error! Reference source not found.**. hese we the primary functions each SOC must have to be called a SOC. The service requirements were identified next. In Section 3.3, a total of 8 service requirements were identified. These are services a SOC could offer either as a MSSP, or alternatively in-house. This led to the determination of the people requirements in Section 3.4. Business requirements were determined next.

The SOC business requirements were derived from the Telecommunications Management Forum's eTOM framework in Chapter 4. After the completion of the SOC requirements, the MoEs had to be determined which will assist in the measuring of the effectiveness and maturity of SOCs. The methodology to determine the MoEs was explained in Section 5.2. A few samples were supplied, and the methodology was applied to the framework. The MoE's for the requirements were neither explicit, nor complete and a typical score was supplied ranging between a score of 0 and 5, with 0 stating the lowest MoE, and 5 the highest MoE. The purpose of this goal was to determine the methodology, and further work is required to populate the rest of these scores.

A scoring mechanism for the maturity of a SOC was then determined based on the SOC requirements, the requirements MoEs and the SOC maturity. These were derived from industry accepted maturity scores in Section 5.1. This allowed for the completion of the third goal, which was to develop a SOC scoring and classification formula in Section 5.3. This classification formula takes into consideration the requirements, the MoE's of the requirements, and maturity of a SOC to derive a score out of 100, where a score of 0 is bad, a score of 50 is average, and a score of 100 is extremely good.

The fourth goal was to design a framework using the Telecommunications Management Forum (TM Forum's) eTOM process Frameworks augmented by ISO/IEC 27001:2005 CoBIT and ITIL. This was achieved in Chapter 4 where all requirements were mapped back to the Telecommunications Management Forum's eTOM framework. More detail is provided on SOC functional requirements, processes and procedures in Appendix C, and Appendix D contains the consolidated SOC framework.

7.4 Conclusion

The author achieved the following goals during the study:

SOC requirements were determined, a scoring and classification mechanism as well as a framework was developed. The goal of developing detailed and complete MoE's were not achieved

The scoring and classification mechanism was previously proposed by the author, and was presented at ISSA 2013. (Jacobs, Arnab, & Irwin, 2013)

After having performed the expert reviews, as well as the classification of local and foreign SOCs, the feedback was that the framework is complete and useful.

The research is significant in that the framework can be used to build and manage SOCs, using a framework based on global, industry accepted standards and frameworks. This allows

for repeatable performance, will lessen the time to operations or market, and allows a baseline for the improvement of existing SOCs and MSSPs service offering.

Using a framework will also directly impact on the cost of establishing a SOC in that the framework makes it unnecessary to go through a learning curve or growth phase. Organisations will much quicker realise return on investment, and will have a fully functional and effective SOC offering which will allow fulfilment of its mandate almost immediately. This directly influences the cost and the security posture of organisations in a positive way.

The significance and benefits to having a classification scheme for SOCs are:

- It allows for a measurement to be done, creating a baseline of the current state of existing SOCs.
- It allows for the identification of gaps, and the improvement of those gaps using the framework.
- It provides a mechanism for prospective SOC services consumers to rate different offerings on maturity and effectiveness, and allows them to become "smart buyers" or smart users" of SOC services.

7.5 Future work

Future work will include the expansion of the requirements MoE's. These would be expanded to include not just a sliding scale, but very specifics, and measurable. Coupled with that, an auditing mechanism needs to be developed to determine an absolute correct score and rating.

The SOC framework in this work is conceptualised. The next steps would be to operationalise the framework, i.e., build a SOC using the framework, and do the validation and verification in this way.

The major technology currently in use by SOCs is a SIEM. There are currently no standards or detailed technical requirements for this tool. Efforts are underway by the ISO/IEC, but this standard is still under development, and does not amount to much (JTC, 2014). The author will be involved in creating this standard.

References

Adler, M. (2007a). CoBIT 4.1. Retrieved May 12, 2013, from http://www.isaca.org/Knowledge-Center/cobit/Documents/COBIT4.pdf

Adler, M. (2007b). CobiT 4.1 Framework. (ITGI, Ed.). Retrieved May 12, 2013, from http://www.isaca.org/Knowledge-Center/cobit/Documents/CobiT_4.1.pdf

Afzaal, M. (2012). A Resilient Architecture for Forensic Storage of Events in Critical Infrastructures. In *2012 IEEE 14th International Symposium on High-Assurance Systems Engineering* (pp. 48 – 55). IEEE. doi:10.1109/HASE.2012.9

Akridge, S. & Chapin, D. A. (2005). How Can Security Be Measured? *Information Systems Audit and Control Association*. Retrieved from http://www.isaca.org/Journal/Past-Issues/2005/Volume-2/Pages/How-Can-Security-Be-Measured.aspx

Al-Mayahi, I. & Mansoor, S. P. (2012). ISO 27001 Gap Analysis - Case Study. In *International Conference on Security and Management*. Retrieved from http://elrond.informatik.tu-freiberg.de/papers/WorldComp2012/SAM9779.pdf

Altech ACS. (2013). Managed Security Services. Retrieved January 21, 2014, from https://www.acs.altech.co.za/managed-security-services

Amoroso, E. G. (2010). *Cyber Attacks: Protecting National Infrastructure*. (Pam Chester, Ed.) (pp. 200 – 201). Butterworth- Heinemann.

Applegate, S. (2009). Social Engineering: Hacking the Wetware! *Information Security Journal: A Global Perspective Volume 18*, *18*(1), 40 – 46.

Arcsight. (2009). Building a Successful Security Operations Center. Retrieved March 13, 2013, from http://www.scribd.com/doc/39599055/ArcSight-Whitepaper-SuccessfulSOC

ATOS Research. (2010). MASSIF. Retrieved May 19, 2013, from http://www.massif-project.eu/description

Ball, E. (2006). Getting to Know ITIL. Retrieved May 17, 2013, from http://www.theiia.org/intAuditor/itaudit/archives/2006/june/getting-to-know-itil/

Bandor, M. (2007). Process and Procedure Definition: A Primer. Retrieved June 17, 2013, from www.sei.cmu.edu/library/assets/process-pro.pdf

Bevis, J. (2012). Creating and Maintaining a SOC - The details behind successful Security Operations Centers. Retrieved August 17, 2013, from http://www.mcafee.com/us/resources/white-papers/foundstone/wp-creating-maintaining-soc.pdf.

Bidou, R. (2004). Security Operation Center Concepts & Implementation. Retrieved April 06, 2013, from http://www.researchgate.net/publication/228587242_Security_Operation_Center_Concepts__Implementation

Blake, J. (2012). Odd SOC's. Retrieved March 12, 2013, from https://jimmyblake.wordpress.com/2012/05/17/the-top-10-mistakes-in-running-a-security-operations-centre/

Broderick, S. (2007). Transforming Your Security Team into a Security Operations Center. Retrieved January 21, 2014, from http://www.infosectoday.com/Articles/SOC.htm

Butler, J. M. (2009). Benchmarking Security Information Event Management (SIEM). Retrieved April 25, 2013, from http://www.sans.org/reading-room/whitepapers/analyst/benchmarking-security-information-event-management-siem-34755

CERT. (2003). Staffing Your Computer Security Incident Response Team – What Basic Skills Are Needed? Retrieved March 02, 2013, from http://www.cert.org/csirts/csirt-staffing.html

Chamelion Security Services. (2013). C180 Security Service. Retrieved January 21, 2014, from http://www.chameleon-ss.com/c180.pdf

Chung, K. (2006). People and Processes More Important than Technology in Securing the Enterprise, According to Global Survey of 4,000 Information Security Professionals. *3rd Annual (ISC)2 Sponsored Global Information Security Workforce Study says Asia-Pacific offers attractive employment incentives and opportunities for information security professionals.* Retrieved September 16, 2014, from https://www.isc2.org/PressReleaseDetails.aspx?id=2714

Cisco Systems. (2006). Cracking the Code for a SOC Blueprint Architecture, Requirements, Methods and Processes and Deliverables. Retrieved January 21, 2014, from ftp://152.33.34.12/CiscoLive/IT Insight/BRKITI-1012.pdf

Cisco Systems. (2007). How to Build Security Operations Center (SOC). Retrieved January 21, 2014, from ftp://ftp-eng.cisco.com/cons/workshops/SP-Powersession-Thailand-Jan-2007/SPSEC-610-Security-Operations-Centers-Basics-Version-2.pdf

Cisco Systems. (2009). Introduction to eTOM. Retrieved September 16, 2014, from http://www.cisco.com/c/en/us/products/collateral/services/high-availability/white_paper_c11-541448.html

Combs, J. (2013). Skills in demand: SOC analysts. *SC Magazine.* Retrieved May 17, 2013, from http://www.scmagazine.com/skills-in-demand-soc-analysts/article/273996/

Curtis, B., Paulk, M., Chrissis, M .B., & Weber, C. (1993). The Capability Maturity Model for Software. Retrieved May 19, 2013, from http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=11955

Del Vecchio, D. (2012). The Security Services a SOC should provide. Retrieved August 06, 2013, from http://www.socstartup.blogspot.it/2012/09/the-security-services-of-soc.html

Dell. (2013). Security Operations Centers. Retrieved January 21, 2014, from http://www.secureworks.com/it_security_services/advantage/soc/

Dempsey, K., Johnson, A., Scholl, M. & Stine, K. (2011). *NIST Special Publication 800-137 Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations.*

Durbin, S. (2012). Information security threats: Building risk resilience. *SearchSecurity*. Retrieved July 02, 2014, from http://searchsecurity.techtarget.com/magazineContent/Information-security-threats-Building-risk-resilience

Ernst & Young. (2013). Security Operations Centers against cybercrime. Retrieved May 17, 2013, from http://www.ey.com/Publication/vwLUAssets/EY_-_Security_Operations_Centers_against_cybercrime/$FILE/EY-SOC-Oct-2013.pdf

Evans, K. & Reeder, R. (2010). A Human Capital Crisis in Cybersecurity: Technical Proficiency Matters - A Report of the CSIS Commission on Cybersecurity for the 44th Presidency. Retrieved April 22, 2013, from http://csis.org/publication/prepublication-a-human-capital-crisis-in-cybersecurity

Fischbach, N. (2008). How to build and run a Security Operations Center. Retrieved June 25, 2013, from www.securite.org/presentations/soc/MEITSEC-SOC-NF-v11.pdf

Furlani, C. (2011). Managing Information Security Risk: Organization, Mission, and Information System View. Retrieved October 20, 2013, from http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf

GetITRight. (2013). ISO27002 Foundation Introduction. Retrieved January 21, 2014, from http://www.getitright.co/ism_course.php

Ghedini, C.G. & Ribeiro, C. (2009). A Framework for Vulnerability Management in Complex Networks. In *International Conference on Ultra Modern Telecommunications & Workshops* (pp. 1 – 8). doi:10.1109/ICUMT.2009.5345578

Guldentops, E. (2007). *COBIT Security Baseline—An Information Security Survival Kit* (2nd ed., pp. 1 – 48). IT Governance Institute (ITGI).

Hardy, G. & Heschl, J. (2008). Aligning COBIT 4.1, ITIL V3 and ISO/IEC 27002 for Business Benefit. ITGI. Retrieved October 21, 2013, from http://www.isaca.org/Knowledge-Center/Research/Documents/Aligning-COBIT,ITILV3,ISO27002-Bus-Benefit-12Nov08-Research.pdf

HCLTech. (2014). HCL Managed Security Services -Security Operations Made Simpler. Retrieved November 21, 2014, from http://www.hcltech.com/it-infrastructure-management/managed-security-services

Hewlett-Packard. (2013). 5G/SOC: SOC Generations. Retrieved January 21, 2014, from http://www8.hp.com/us/en/software-solutions/software.html?compURI=1343719#!

HP Enterprise Security Business. (2009). Building a successful Security Operations Center. Retrieved January 21, 2014, from http://h71028.www7.hp.com/enterprise/downloads/software/ESP-BWP014-052809-09.pdf

Hutchins, E. M. (2010). Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. Retrieved November 22, 2013, from http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf.

IBM. (2008). Control Objectives for Information and related Technology (CobiT®) Internationally accepted Gold standard for IT Controls & Governance. Retrieved January

21, 2014, from http://www-304.ibm.com/industries/publicsector/fileserve?contentid=187551

IBM. (2104). Virtual Security Operations Center (SOC). Retrieved January 21, 2014, from http://www-935.ibm.com/services/us/en/it-services/virtual-security-operations-center-soc.html

INCOSE. (2010). *Systems Engineering Handbook: A Guide for System Life Cycle processes and activities v3.2.* (C. Haskins, Ed.) (pp. 7 – 17). Retrieved from www.incose.org/ProductsPubs/Doc/IS2010_SEHandbookv3_2_Paper.pdf

ISACA. (1996). CoBIT DS13.3 - IT Infrastructure Monitoring. Retrieved January 21, 2014, from http://www.isaca.org/Groups/Professional-English/ds13-3-it-infrastructure-monitoring/Pages/Overview.aspx

ISACA. (2006). Imperatives Driving Security Convergence. *Information Systems Control Journal*, *4*. Retrieved from http://www.isaca.org/Journal/Past-Issues/2006/Volume-4/Pages/Imperatives-Driving-Security-Convergence1.aspx

ISACA. (2013). CoBIT 5 for Information Security. Retrieved January 21, 2014, from http://www.isaca.org/COBIT/Documents/COBIT-5-for-Information-Security-Introduction.pdf

ISecT. (2011). Information security frameworks from "Audit" to "Zachman." Retrieved January 21, 2014, from www.iso27001security.com/IsecT_white_paper_on_security_frameworks_A_to_Z.pdf

ISO / IEC. (2005). ISO/IEC 27001:2005 Information technology -- Security techniques -- Information security management systems -- Requirements. ISO / IEC. Retrieved January 21, 2014, from http://www.iso.org/iso/catalogue_detail?csnumber=42103

ISO / IEC. (2008). ISO/IEC 15288:2008. Retrieved January 21, 2014, from http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=43564

ISO / IEC. (2009). An Introduction to ISO 27001, ISO 27002....ISO 27008. Retrieved January 21, 2014, from http://www.27000.org/

ITGovernanceUSA. (2011). ITIL®– IT Infrastructure Library® & IT Service Management. Retrieved January 21, 2014, from http://www.itgovernanceusa.com/itil.aspx

Jacobs, P., Arnab, A., & Irwin, B. (2013). Classification of Security Operation Centers. In *Information Security for South Africa, 2013* (pp. 1 – 7). doi:10.1109/ISSA.2013.6641054

Jansen, W. (2009). *Directions in Security Metrics Research*. *NIST* (Vol. NISTIR 756, pp. 1 – 26). Retrieved from http://csrc.nist.gov/publications/nistir/ir7564/nistir-7564_metrics-research.pdf

Jiejin, H. (2009). *A Practical Approach to the Operation of Telecommunication Services driven by the TMF eTOM Framework - A thesis submitted for the degree of Master of Universitat Politècnica de Catalunya*. Universitat Politècnica de Catalunya.

JTC, I. (2014). ISO/IEC WD 27044 Guidelines for Security Information and Event Management (SIEM). Retrieved January 21, 2014, from http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=62287

Kelley, D. & Moritz, R. (2006). Best Practices for Building a Security Operations Center. *Information Systems Security*, *14*(6), 27–32. doi:10.1201/1086.1065898X/45782.14.6.20060101/91856.6

Knowledgetransfer. (2011a). ITIL OLA Definition. Retrieved from http://www.knowledgetransfer.net/dictionary/ITIL/en/Operational_Level_Agreement.htm

Knowledgetransfer. (2011b). ITIL SLA Definition. Retrieved June 27, 2014, from http://www.knowledgetransfer.net/dictionary/ITIL/en/Service_Level_Agreement.htm

Krygiel, A. J. (1999). Behind the Wizard's Curtain: An Integration Environment for a System of Systems. CCRP publication series. Retrieved March 20, 2013, from http://www.dodccrp.org/files/Krygiel_Wizards.pdf

Lemos, R. (2012). Do You Need A Security Operations Center? *Tech Center: Security Monitoring*. Retrieved April 13, 2013, from http://www.darkreading.com/security-monitoring/167901086/security/perimeter-security/232500661/do-you-need-a-security-operations-center.html

Lew, D. (2009, July). COBIT Focus. Retrieved October 22, 2013, from http://www.isaca.org/knowledge-center/cobit/documents/cobit-focus-vol-3-2009.pdf

Locke, G. (2010). NIST Special Publication 800-53 Revision 3 - Recommended Security Controls for Federal Information Systems and Organizations. *NIST Special Publication*. Retrieved March 12, 2013, from http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf

M. Nicolett. (2012). *Critical Capabilities for Security Information and Event Management*. Retrieved from https://www.gartner.com/doc/2022315/critical-capabilities-security-information-event

MacDonald, I. (2010). ITIL Process Assessment Framework. Retrieved January 21, 2014, from http://www.itsmfi.org/files/ITIL Process Assessment Framework - MacDonald.pdf

Madani, A., Rezayi, S. & Gharaee, H. (2011). Log Management comprehensive architecture in Security Operation Center (SOC). *2011 International Conference on Computational Aspects of Social Networks (CASoN)*, 284 – 289. doi:10.1109/CASON.2011.6085959

Maitland, C. & Thomas, H. F. (2012). Internet censorship circumvention technology use in human rights organizations: an exploratory analysis. Retrieved June 21, 2013, from http://cmaitland.ist.psu.edu/wp-content/uploads/2012/10/MaitlandCensorshipJIT2012.pdf.

McAfee. (2010). McAfee's Unique Prevent-Detect-Respond Approach and Security Operations Center Showcase Best Practices. Retrieved January 21, 2014, from https://www.mcafeetheplace.com/moc/docs/cs_soc_1010_fnl_hires.pdf

McAfee. (2012). Focus on 5 SIEM Requirements. Retrieved January 21, 2014, from http://www.mcafee.com/us/resources/brochures/br-focus-on-five-siem-requirements.pdf

Milham, D. (2004). How can the eTOM Framework help Service Providers in today's market pIace? *Network Operations and Management Symposium*, *Volume 2*, 59 – 71. doi:10.1109/NOMS.2004.1317641

Milne, J. (2005). Build Your Own Security Operations Center. *InformationWeek*. Retrieved June 17, 2013, from http://www.informationweek.com/build-your-own-security-operations-cente/167100524

MindPoint Group LLC. (2011). Security Operations Center (SOC) Implementing Security Monito ring in Small and Mid-sized Organizations. Retrieved January 21, 2014, from http://www.mindpointgroup.com/SOC.pdf

MyBroadband. (20113). COBIT 5 makes enterprise architecture a mandatory discipline. Retrieved January 21, 2014, from http://companies.mybroadband.co.za/blog/2013/04/29/cobit-5-makes-enterprise-architecture-a-mandatory-discipline/

Nakashima, E. & Krebs, B. (2009). As attacks increase, U.S. struggles to recruit computer security experts. Retrieved August 08, 2013, from http://www.distributedworkplace.com/DW/Government/Government 2009/As attacks increase US struggles to recruit computer security experts.doc

Nicho, M. (2012). Incorporating COBIT Best Practices in PCI DSS V2.0 for Effective Compliance. *ISACA Journal*, *1*. Retrieved from http://www.isaca.org/Journal/Past-Issues/2012/Volume-1/Pages/Incorporating-COBIT-Best-Practices-in-PCI-DSS-V2-0-for-Effective-Compliance.aspx

Nickle, M. (2011). Best Practices for Building a Security Operations Center - Untangling the Mess Created by Multiple Security Solutions. Retrieved January 21, 2014, from http://www.slideshare.net/nickle4245/soc-presentation-10590459

NIST. (2012). Security Maturity Levels. Retrieved January 21, 2014, from http://csrc.nist.gov/groups/SMA/prisma/security_maturity_levels.html

Northcutt, S. (2009). Security Controls. Retrieved January 21, 2014, from http://www.sans.edu/research/security-laboratory/article/security-controls

NoxGlobe. (2011). ITIL v3 Processes. Retrieved January 21, 2014, from http://www.noxglobe.com/blog/itil/itil-v3-processes/

Office of Government Commerce. (2000). ITIL. Retrieved January 21, 2014, from http://www.itil-officialsite.com/

Oxford University Press. (2011). Oxford Advanced Learner's Dictionary. Retrieved January 21, 2014, from http://oald8.oxfordlearnersdictionaries.com/

PCI Security Standards Council. (2010). Payment Card Industry (PCI) Data Security Standards Overview. Retrieved January 21, 2014, from https://www.pcisecuritystandards.org/security_standards/

Pederiva, A. (2003). The COBIT Maturity Model in a Vendor Evaluation Case. *Information Systems Control Journal*, *3*(26-29). Retrieved from http://www.isaca.org/Journal/Past-Issues/2003/Volume-3/Documents/jpdf033-COBITMaturityModel.pdf

Phillips, M. (2003). Using a Capability Maturity Model to Derive Security Requirements. Retrieved June 19, 2013, from http://www.sans.org/reading_room/whitepapers/bestprac/capability-maturity-model-derive-security-requirements_1005

Protz, M. (2005). A SAS® Framework for Network Security Intelligence. In *SUGI 30* (Vol. Paper 190-, pp. 1–16). Retrieved from http://www2.sas.com/proceedings/sugi30/190-30.pdf

Qualys. (2012). QualysGuard Vulnerability Management and Remediation FAQ. Retrieved January 21, 2014, from http://www.qualys.com/support/faq/vulnerability/

Razieh Sheikhpour, N. M. (2012). A best practice approach for integration of ITIL and ISO/IEC 27001 services for information security management. *Indian Journal of Science and Technology*, *5*(2). Retrieved from http://www.indjst.org/index.php/indjst/article/download/30359/26290

Reply Communication Valley. (2011). Security Operations Center. Retrieved January 21, 2014, from http://www.reply.eu/1937_img_COMVR11_SOC_eng

Roedler, G. J. & Jones, C. (2005). *Technical Measurement*. *INCOSE-TP-2003-020-01 (2005)* (pp. 9 – 10). INCOSE. doi:INCOSE-TP-2003-020-01

Roth, I. (2008). ITIL Overview. Retrieved July 18, 2013, from http://www.itilcertification.org/

Rothke, B. (2009). Building a Security Operations Center (SOC). *RSA Conference Europe 2009*. RSA Security Inc. Retrieved June 17, 2013, from https://365.rsaconference.com/servlet/JiveServlet/previewBody/2120-102-2-2585/NET-208 - Building a Security Operations Center (SOC).pdf

RSA. (2011). Creating an Effective Security Operations Function. Retrieved January 21, 2091, from http://www.comprosec.ch/fileadmin/document_archive/Library/RSA_enVision/WPE_Creating_an_Effective_Security_Operations_Function___9558_SOC_WP_0808-lowres_cps_dis.pdf

RSA. (2013a). Building an Intelligence-Driven Security Operation Center. Retrieved January 21, 2014, from http://www.emc.com/collateral/technical-documentation/h11533-intelligence-driven-security-ops-center.pdf

RSA. (2013b). RSA Launches RSA NextGen Security Operations Services to Help Customers Build Battle-Ready Cyber Defenses. Retrieved January 21, 2014, from http://www.emc.com/about/news/press/2013/20130225-02.htm

Sahibudin, S., Sharifi, M, & Ayat, M. (2008). Combining ITIL, COBIT and ISO/IEC 27002 in Order to Design a Comprehensive IT Framework in Organizations. *2008 Second Asia International Conference on Modelling Simulation (AMS) (2008)*, 749. doi:10.1109/AMS.2008.145

Sajko, M. (2007). Measuring and Evaluating the Effectiveness of Information Security. Retrieved January 21, 2014, from http://www.academypublish.org/papers/pdf/310.pdf

Sameer Paradia. (2012). Enterprise Sertrvice Operation Center. Retrieved from http://www.slideshare.net/sameerparadia/it-enterprise-service-operation-center

SANS Institute. (2011). Security Predictions 2012 & 2013 - The Emerging Security Threat. Retrieved January 21, 2014, from http://www.sans.edu/research/security-laboratory/article/security-predict2011

SANS Institute. (2013). Critical Controls for Effective Cyber Defense V 4.1. Retrieved January 21, 2014, from http://www.sans.org/critical-security-controls/cag4-1.pdf

SecureOps. (2013). SecureOps Security Operations Center. Retrieved January 21, 2014, from http://secureops.com/Services/Monitoring-Services.html

Shenk, J. (2011). SANS Seventh Annual Log Management Survey Report. Retrieved May 19, 2013, from http://www.sans.org/reading_room/analysts_program/logmgt-survey-web.pdf

South African Government. (2002). Electronic Communications and Transactions Act, 2002 (Act No. 25 of 2002). Retrieved January 21, 2014, from http://www.acts.co.za/electronic-communications-and-transactions-act-2002/

Spafford, G., Wheeler, A. J. & Mingay, S. (2012). Updates in COBIT 5 Aim for Greater Relevance to Wider Business Audience. Retrieved July 17, 2013, from https://www.gartner.com/doc/1982323

Suer, M. (2012). 4 reasons COBIT 5 should be part of your IT strategy. Retrieved April 14, 2013, from http://www.enterprisecioforum.com/en/blogs/mylessuer/4-reasons-cobit-5-should-be-part-your-it

Swift, D. (2010). Successful SIEM and Log Management Strategies for Audit and Compliance. Retrieved November 29, 2013, from http://www.sans.org/reading_room/whitepapers/auditing/successful-siem-log-management-strategies-audit-compliance_33528.

Symantec. (2012). Symantec Unveils New Global Security Operations Center in U.S. Retrieved November 21, 2013, from http://www.symantec.com/about/news/release/article.jsp?prid=20120207_01

System Integrity. (2010). Control Objectives for Information and and related Technology. Retrieved June 30, 2014, from http://systemi.ca/audit/cobit

Tenable Network Security. (2012). SANS 2007 Top 20 Scanning and Report Policies. Retrieved from http://blog.tenablesecurity.com/2007/12/sans-2007-top-2.html

Thanh Viet Do. (2003). Global Information Assurance Certification Paper. Retrieved January 21, 2014, from http://www.giac.org/paper/gslc/18/federal-security-training-requirements/105108

TMForum. (2013). Business Process Framework. Retrieved January 21, 2014, from http://www.tmforum.org/BusinessProcessFramework/1647/home.html

T-Systems. (2013). Security. Retrieved January 21, 2014, from http://www.t-systems.com/cebit/cyber-defense-strategies-and-secure-mobile-communication-by-t-systems/1033478

United States Government. (2002). The Sarbanes-Oxley Act of 2002. Retrieved January 21, 2014, from http://www.soxlaw.com/s404.htm

Von Solms, R., & Posthumus, S. (2004). A framework for the governance of information security. *Computers & Security*, *23*(8), 638 – 646. doi:10.5171/2011.726196

Wallhoff, J. (2005). ITIL Security Management. Retrieved January 21, 2014, from http://www.scillani.se/assets/pdf/Scillani Presentation ITIL Security Managment.pdf

Wang, J. (2010). Anatomy of a Security Operations Center. Retrieved November 30, 2013, from http://www.us-cert.gov/sites/default/files/gfirst/presentations/2010/Incident_Management_Anatomy_of_a_Security_Operations_Center.pdf

Warda, K. (2005). A Fundamental and Essential look into Managed Security Services. *SANS (GSEC) Practical Assignment Version 1.4c – Option 1 March 28, 2005*. Retrieved April 12, 2013, from http://www.giac.org/paper/gsec/4432/fundamental-essential-managed-security-services/107412

Warren, K. . . . (2010). Security Controls in Service Management. Retrieved June 21, 2013, from http://www.sans.org/reading_room/whitepapers/iso17799/security-controls-service-management_33558

Weil, S. (2010). How ITIL Can Improve Information Security. Retrieved January 21, 2014, from http://www.symantec.com/connect/articles/how-itil-can-improve-information-security

Willet, K. (2008). How to Achieve 27001 Certification. Retrieved April 12, 2013, from http://www.sos.cs.ru.nl/applications/courses/sio2009/literatuur/How to Achieve 27001 Certification (2007).pdf

Yuan, S. & Zou, C. (2011). The Security Operations Center Based on Correlation Analysis. *2011 IEEE 3rd International Conference on Communication Software and Networks (2011)*, 334 – 337. doi:10.1109/ICCSN.2011.6013727

Appendix A

List of Abbreviations

BSI	British Standards Institute
CoBIT	Control Objectives for Information Technology
COTS	Commercial Off The Shelf
CSIRT	Computer Security Incident Response Team
DDoS	Distributed Denial of Service
eTOM	enhanced Telecom Operations Map
GRC	Governance, Risk and Compliance
IT	Information Technology
IDS	Intrusion Detection System
ISACA	Information Systems Audit and Control Association
ISO	Industry Standards Organisation
IPS	Intrusion Prevention System
IT	Information Technology
ITGI	IT Governance Institute
ITIL	Information Technology Infrastructure Library
ITSMF	IT Service Management Forum
INCOSE	International Council of Systems Engineering
NGOSS	New Generation Operations Systems and Software
MoE	Measure of Effectiveness
MSSP	Managed Security Service Provider
NIST	National Institute of Standards and Technology
NOC	Network Operations Center
ROI	Return on Investment
SAS	Statement on Auditing Standards
SANS	**S**ysAdmin **A**udit **N**etworking and **S**ecurity
SEI	Software Engineering Institute
SOC	Security Operations Center
SIEM	Security Incident and Event Monitoring
TAM	Telecom Application Map
TM Forum	Telecommunications Management Forum
TMF	Telecommunications Management Forum
TMN	Telecommunications Management Network
TNA	Technology Neutral Architecture
TOM	Telecom Operations Map

Appendix B

The need for SOC Functions and Monitoring

All Information Security Frameworks and Standards highlight the need for the monitoring of security controls, which can be fulfilled by the Event Log Collection and Management service in a SOC. The latter can also provide guidance on policies, processes and controls that an organisation or service provider should have.

ISO/IEC 27002 -10.10 (ISO/IEC, 2009) states that *"Systems should be monitored and information security events should be recorded. Operator logs and fault logging should be used to ensure that information system problems are identified."*

The National Institute of Standards and Technology (NIST) describes monitoring in Special Publication (SP800-137) (Dempsey, Johnson, Scholl, & Stine, 2011) as "maintaining ongoing awareness of information security, vulnerabilities, and threats to support organisational risk management decisions"

NIST SP 800-39 (Furlani, 2011) mentions three key activities when monitoring. These are:

- Monitoring for effectiveness;
- Monitoring for change to systems and environments of operation; and
- Monitoring for compliance.

The necessity for monitoring and Incident Management is also highlighted in the SANS Critical Controls Version 4.1 of 2013 (SANS Institute, 2013), which stresses the continuous monitoring of security measures in order to test and validate their effectiveness, as well as the NIST SP800-53 (Recommended Security Controls for Federal Information Systems and organisations) (Locke, 2010), which describe the process for selecting and specifying security controls to be monitored.

Table B-7-1: Monitoring requirements as expressed by major Standards and Frameworks shows the relationship across SANS, CoBIT, ITIL and ISO/IEC 27001:2005 (Hardy & Heschl, 2008), which expresses the requirements for the active management of IT Security, monitoring of future trends and regulations, independent review of information security and security incident management. From this it is clear that the functional requirements as specified, including monitoring to detect attacks and to ensure compliance and effectiveness, are a requirement by NIST, CoBIT, ISO/IEC 27001:2005 and ITIL.

Table B-7-1: Monitoring requirements as expressed by major Standards and Frameworks

CobiT 4.1 Control Objective[1]	Key Areas	ITIL V3 Supporting Information[2]	ISO/IEC 27002:2005[3] Supporting Information	SANS Critical Controls[4]	NIST SP800-53[5]
PO3.3 Monitor future trends and regulations	• Business sector, industry, technology, infrastructure, legal and regulatory trends	• SS 2.4 Principles of service management • SD 4.3.5.7 Modelling and trending	• 6.1.1 Management commitment to information security		
DS5.1 Management of IT security	• High-level placement of security management to meet business needs	• SD 4.6 Information security management • SO 5.13 Information security management and service operation	• 6.1.1 Management commitment to information security • 6.1.2 Information security co-ordination • 6.2.3 Addressing security in third party agreements • 8.2.2 Information security awareness, education and training		
DS5.3 Identity management	• Identification of all users (internal, external and temporary) and their activity	•SO 4.5 Access management	• 11.2.3 User password management • 11.3.1 Password use • 11.4.1 Policy on use of network services • 11.5.1 Secure logon procedures • 11.5.2 User identification and authentication • 11.5.3 Password management system • 11.5.5 Session time-out • 11.5.6 Limitation of connection time • 11.6.1 Information access restriction	Critical Control 15: Controlled Access Based on the Need to Know	AC-1, AC-2 (b, c), AC-3 (4), AC-4, AC-6, MP-3, RA-2 (a)
DS5.4 User account management	• Life cycle management of user accounts and access privileges	• SO 4.5 Access management • SO 4.5.5.1 Requesting access • SO 4.5.5.2 Verification • SO 4.5.5.3 Providing rights • SO 4.5.5.4 Monitoring identity status • SO 4.5.5.5 Logging and tracking access • SO 4.5.5.6 Removing or restricting rights	• 6.1.5 Confidentiality agreements • 6.2.1 Identification of risks related to external parties • 6.2.2 Addressing security when dealing with customers • 8.1.1 Roles and responsibilities • 8.3.1 Termination responsibilities • 8.3.3 Removal of access rights • 10.1.3 Segregation of duties • 11.1.1 Access control policy • 11.2.1 User registration • 11.2.2 Privilege management • 11.2.4 Review of user access rights • 11.3.1 Password use • 11.5.1 Secure logon procedures • 11.5.3 Password management system • 11.6.1 Information access restriction	Critical Control 12: Controlled Use of Administrative Privileges	AC-6 (2, 5), AC-17 (3), AC-19, AU-2 (4)
DS5.5 Security testing, surveillance and monitoring	• Proactive testing of security implementation	• SO 4.5.5.6 Removing or restricting rights	• 6.1.8 Independent review of information security	Critical Control 4: Continuous	RA-3 (a, b, c, d), RA-5 (a, b, 1, 2, 5, 6)

	• Timely accreditation • Timely reporting of unusual events	• SO 5.13 Information security management and service operation	• 10.10.2 Monitoring system use • 10.10.3 Protection of log information • 10.10.4 Administrator and operator logs • 12.6.1 Control of technical vulnerabilities • 13.1.2 Reporting security weaknesses • 15.2.2 Technical compliance checking • 15.3.1 Information systems audit controls	Vulnerability Assessment and Remediation Critical Control 20: Penetration Tests and Red Team Exercises	CA-2 (1, 2), CA-7 (1, 2), RA-3, RA-5 (4, 9), SA-12 (7)
DS5.6 Security incident definition	• Definition and classification of security incident characteristics	• SD 4.6.5.1 Security controls (high-level coverage, not in detail) • SD 4.6.5.2 Management of security breaches and incidents	• 8.2.3 Disciplinary process • 13.1.1 Reporting information security events • 13.1.2 Reporting security weaknesses • 13.2.1 Responsibilities and procedures • 13.2.3 Collection of evidence	Critical Control 18: Incident Response and Management	IR-1, IR-2 (1), IR-4, IR-5, IR-6 (a), IR-8
DS5.7 Protection of security technology	• Resistance to tampering	• SO 5.4 Server management and support	• 6.1.4 Authorisation process for information processing facilities • 9.1.6 Public access, delivery and loading areas • 9.2.1 Equipment siting and protection • 9.2.3 Cabling security • 10.6.2 Security of network services • 10.7.4 Security of system documentation • 10.10.1 Audit logging • 10.10.3 Protection of log information • 10.10.4 Administrator and operator logs • 10.10.5 Fault logging • 10.10.6 Clock synchronisation • 11.3.2 Unattended user equipment • 11.3.3 Clear desk and clear screen policy • 11.4.3 Equipment identification in networks • 11.4.4 Remote diagnostic and configuration port protection		
ME1.2 Definition and collection of monitoring data	• Balanced set of objectives approved by stakeholders • Benchmarks, availability and collection of measurable data	• SD 4.2.5.10 Complaints and compliments • CSI 4.1c Step three—Gathering data • CSI 4.1d Step four—Processing the data	• 10.10.2 Monitoring system use	Critical Control 14: Maintenance, Monitoring, and Analysis of Security Audit Logs	AC-17 (1), AC-19, AU-2 (4), AU-3 (1,2), AU-4, AU-5, AU-6 (a, 1, 5), AU-8, AU-9 (1, 2), AU-12 (2), SI-4 (8)

[1] Taken from CoBIT (Adler, 2007b)
[2] Taken from ITIL (Office of Government Commerce, 2000)
[3] Taken from ISO/IEC 27001:2005 (ISO / IEC, 2005)
[4] Taken from SANS Critical Controls (SANS Institute, 2013)
[5] Taken from NIST SP 800-53 (Locke, 2010)

Appendix C

SOC Functional requirements, Processes and Procedures

The SOC functional requirements are captured, with the processes and procedures. This serves as a reference guide to all processes and procedures needed when starting a SOC. The diagram only states which processes and procedures are needed, but does not include the details or any templates.

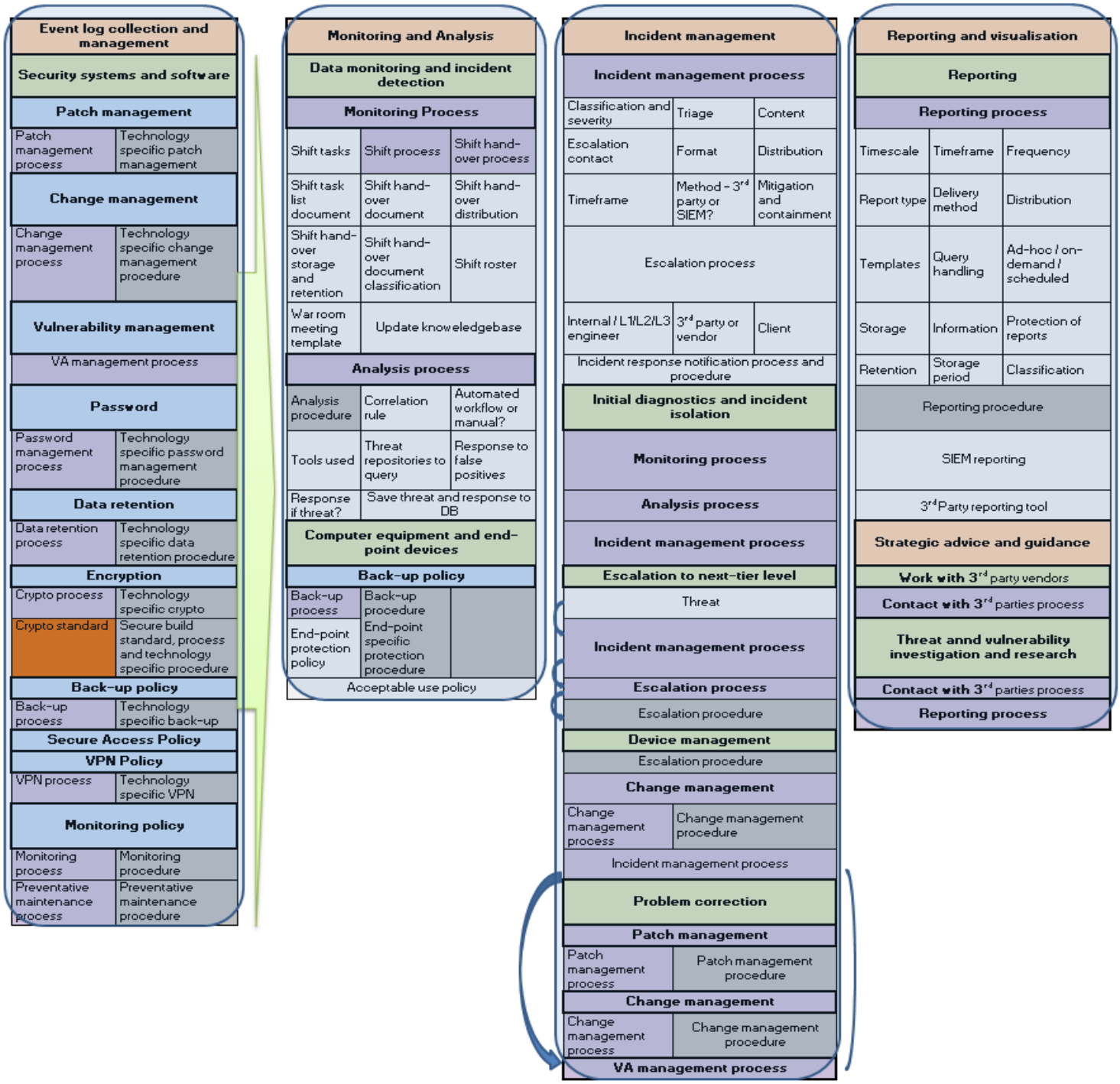

Figure 7-1: SOC Functional requirements, Processes and Procedures

Appendix D

SOC Consolidated Framework

The SOC consolidated framework is a collection of all the requirements mapped back to the eTOM framework. The consolidated framework includes the supporting standards, frameworks and best practices which supports the selection of the requirements.

The framework further includes all processes and procedures needed to build and run a SOC. Due to the size and volume, the framework was divided into three portions, Strategy, Infrastructure and Product, Operations and Enterprise management

Strategy, Infrastructure and Product

Standard, Reference, Framework	Procedure	Process	Policy	Deliverable	Strategy and Commit	Infrastructure Lifecycle Management	Product Lifecycle Management
					Marketing and Offer Management		
					Market and strategy policy 1.2.1.1 Gather and analyse market information 1.2.1.1.1 Gather and analyse product information 1.2.1.2.1	Product and offer capability delivery 1.2.1.3 Define product capability requirements 1.2.1.3.1 Capture product infrastructure requirements 1.2.1.3.1.1	Product offer development and retirement 1.2.1.5 Gather and analyse new product ideas 1.2.1.5.1, 1.2.1.5.1.2 and 1.2.1.5.3 Product marketing, communication and promotion 1.2.1.7 Develop product and campaign message 1.2.1.7.2 Apply product business case 1.2.1.3.3, 1.2.1.3.3.1 and 1.2.1.3.3.2 Sales development 1.2.1.6 Develop sales and channel proposals 1.2.1.6.2 Develop product commercialisation strategy 1.2.1.5.4
					Service Development and Management		
CoBIT PO1.4, 1,6 ITIL SS3.5, 3.5.4.1, 4.4, 5.5, 6.5, SD3.6.2					Establish service strategy and goals 1.2.2.1.3 Define service support strategies 1.2.2.1.4	Service capability and delivery 1.2.2.2.6 Enable service support and operations 1.2.2.2.5, 1.2.2.2.5.2, 1.2.2.2.5.3	
					Resource Development and Management		
						None	
					Supply Chain Development and Management		
						None	

Figure 7-2: SOC Consolidate framework: Strategy, Infrastructure and Product

Operations

Standard, Reference, Framework	Procedure	Process	Policy	Deliverable	Operations, Support and Readiness	Fulfilment	Assurance	Billing and Revenue Management
						Customer Relationship Management		
CoBIT DS8.5, DS10.1 - 10.4 ITIL SO4.1.5.9, 4.5.5.1 - 4.5.5.8 ISO\IEC 27001:2005		*Problem handling *Asset classification process	*Asset management policy *Asset classification policy	Sales proposal and collateral		Selling 1.1.1.4 Develop sales proposal 1.1.1.4.6	Problem handling 1.1.1.6 Customer QoS / SLA management 1.1.1.7	
						Service Management and Operations		
CoBIT PO1.3, 2.2,8.2, 8.6, DS9.2, 9.3 ITIL SS4.4, 7.5, ST3.2, 4.1.5.2, 4.3.5.3 - 4.3.5.6, 4.5, SD5.2, SO 5.4, 7 ISO\IEC 27001:2005 7.1.1, 7.1.2, 7.2.2, 10.7.4, 11.4.3, 12.4.2, 12.5.3, 12.6.1, 15.1.5		Take-on process		Take-on template	SMO support ad readiness 1.1.2.1 Manage service inventory 1.1.2.1.1 Support service problem management 1.1.2.1.3		Service quality management 1.1.2.4 Monitor service quality 1.1.2.4.1 Resource performance management 1.1.3.4 Monitor resource performance 1.1.3.4.1 Control resource performance 1.1.3.4.3	
						Resource Management and Operations		
		*Shift hand over *WAR Room *Recruitment process (skills etc)	Shift policy	*Shift roster *WAR Room template *Shift hand-over template	Workforce management 1.1.3.7 Manage schedules and appointments 1.1.3.7.1 Determine work schedule 1.1.3.7.1.2			
						Supplier / Partner Relationship Management		
CoBIT DS2.2 ITIL SD4.2.5.9, 4.7.5.2, 4.7.5.4 - 4.7.5.5 ISO\IEC 27001:2005 6.2.3, 10.2.3,				*SLA *Escalation contact list			Supplier / Partner relationship management 1.1.4 Supplier / Partner problem reporting and management 1.1.4.3	

Figure 7-3: SOC Consolidate framework: Operations

Enterprise Management

Standard, Reference, Framework	Procedure	Process	Policy	Deliverable	
					Strategy and Enterprise Planning
ITIL ST4.2 CoBIT AI6 ISO\IEC 27001:2005 10.1.2, 12.5.3	Technology specific change management procedure	Change management process CAB process	Change management policy	Request for change document	Strategic business planning 1.3.1.1 Business development 1.3.1.2 Develop concepts for revenue streams 1.3.1.2.1 Group enterprise management 1.3.1.4
					Enterprise Risk Management
CoBIT DS4.1, 4.2, 4.4, 5.1, 5.5, 5.6, 8.2, 8.3 - 4, 10.1 PO 3.3, 4.8, 6.1 - 6.2, 6.4 ITIL SD4.5, 4.5.1, 4.5.5.2 - 4.5.5.4, 4.6, 5.1 - 2, 5.13, 6.4, SO4.1.5.8, 4.1.5.1, 4.2, 4.2.5.1 - 4.2.5.9, 5.9, CSI 5.6.3,	Incident analysis and investigation procedure	*IT DR process *Policy review process *Incident management process *Call logging process *Escalation process *Incident analysis and investigation process *Incident report	*Log protection policy and process *VA management policy *InfoSec policy document *Policy on use of network services *Clear desk and screen policy *Access control policy	*BC framework and plan *BC testing and training plan *VA management strategy *Monitoring policy health, threats, capacity etc) *VA and other reports *ISMS or SCF *Incident classification	Business continuity management 1.3.2.2 Manage proactive security management 1.3.2.2.1 Define security management prevention 1.3.2.2.8 Monitor industry trends for security management 1.3.2.2.2 Define monitoring to facilitate security management 1.3.2.2.9 Define security management policies and procedures 1.3.2.2.3 Define security management analysis 1.3.2.2.10
					Financial and Asset Management
CoBIT PO2.2, 5.1, DS6.1 - 3, 9.2 - 3 ITIL SS3.1, 5.1, 5.3 - 4, SD5.2, 7, ST 4.1.5.2 - 6, SO5.4, 7		*Accounting process *Asset return process	Acceptable use of assets	*Cost modelling and charging *Asset inventory *Asset identification and classification	Financial management 1.3.5.1 Asset management 1.3.5.2
					Enterprise Effectiveness Management
					ITIL incident management 1.3.3.9
					Stakeholder and External Relations Management
CoBIT DS1.1, 2.2, 3, 3.1 5, 13.2 - 3, 5, 6, 8.18.1, AI1.1, 2.2, 5.2, PO3.3, 4.15, 8.4 - 5 ITIL SO4.2.1.4 - 5, 7 - 8, SS2.6, 4.3 - 4, 7.2 - 3, 5, SD4.2.1, 4.2.5.1 - 10, SD 4.3.5.1, 4.3.4.1, 4.3.5.1, 4.3.4.2, 4.3.5.2, 4.3.4.3, 4.3.5 - 8, 4.3.8, CSI5.6.2 ISO\IEC 27001:2005		*Service level monitoring process *SLA management process *Threshold management and control process *Capacity management process *Optimisation process *Demand management		*Service level management framework *Service level reports *Capacity management report *SLA's *Capacity plan *Event reporting and trend analysis	Corporate communications and image management 1.3.6.1 Regulatory management
					Human Resources Management
CoBIT PO7.1 - 8 ITIL SD6.3 ISO\IEC 27001:2005 8.1.1 - 3, 8.3.3 - 3		*Shift handover *KPI management *Recruitment process *Termination process		*Shift roster *Shift duty sheet Shift task list *WAR Room agenda *Roles and responsibilities	HR policies and practices 1.3.7.1 Facilitate performance appraisal 1.3.7.1.1 Facilitate remuneration policies and levels 1.3.7.1.1 Facilitate allowances and benefits 1.3.1.7.2 Facilitate occupational health and safety 1.3.7.1.3
					Knowledge and Resource Management
CoBIT AI4.2 - 4.4, PC1, PO2.1, 4 ITIL ST4.7.1, 4.7.4.1, 4.7.5.1 - 3, 4.7.7.1, .7.4.2, 4.7.5.4, 4.7.7.2 - 3, 4.4.5.8, 4.4, 4.5		Knowledge transfer to business and end-users		Service knowledge management system	Knowledge management 1.3.4.1 ITIL service level management 1.3.3.10

Figure 7-4: Figure 7 3: SOC Consolidate framework: Enterprise Management

Appendix E

SOC Functional Requirements and scoring sheet

This section contains the SOC scoring sheet in Excel format. The functional requirements with their MoEs and maturity ratings are captured here. The sheet uses a formula to calculate the SOC final score. An explanation for each MoE is given, but only from a low and high score perspective, such as, "*a SOC with a low capability will do or have…"*, and "*a SOC with a high capability will do or have…"* detailed MoEs will be determined during further studies. The SOC functional requirements and scoring sheet can be publically accessed from this link: https://docs.google.com/spreadsheets/d/1uk1mINPMjhv9YTxt4xKQm6F1qYIVjq4u84vcD0kSO10/edit?usp=sharing

The SOC functional requirements can also be accessed by "double clicking" the icon 

Appendix F

Expert Reviewer's Detailed Comments

Expert Reviewer # 1 Dr Andrew Hutchison

Dr Hutchison works at T-Systems as leading the global Security Offering team. In addition to numerous management positions within T-Systems (in South Africa as well as in the global organisation), he has been instrumental in defining the security offerings for T-Systems, including SOC services. Dr Hutchison is also an Adjunct Professor at the University of Cape Town, and has been a participant in the MASSIF project, which investigates solutions for next-generation SIEM technologies. Thus, we believe that he has the experience and expertise to review the proposed solution.

The framework should be grouped to mimic the ITIL "Plan, Build and Run" aspects.

The framework should be simplified, and over-complication should be avoided.

Services and functional requirements should be reviewed to determine which ones are core to a SOC, and which ones are complementary to SOC.

Most SOCs have a one-dimensional view. We need to ensure that SOCs provide three-dimensional views. An example would be to ensure that SOC incident management ties in and integrates with the organisation incident management tools, processes and procedures. This is not reflected in the framework.

We also need to determine aspects that differentiate between a SOC and next-generation SOC, and make sure that the framework caters for next-generation SOCs as well. Next-generation SOCs are defined in this thesis, and their requirements have been addressed.

Remarks are further broken down per requirement:

Analysis ability:

A SOC with a high capability will offer real-time monitoring, assisted by correlation rules and automated workflows on a 24x7x365 basis. Specialist analysts are appointed for most systems in scope. Near real-time analysis is offered.

Remark: The remark was made that we are mixing up different aspects. Analysis ability is almost a service issue. We need to break up and clarify these aspects. It should be more refined (call it reactive/proactive/correlation/big data/data mining). Qualitative aspects need to be considered. Timing should be removed. Analysis capability depends on techniques; timing is a services issue.

Reporting and visualisation:

Meaningfulness of reports needs to be included as a measure of effectiveness. It could be broken down into interpretation and analysis of reports before submission to clients. Reporting and visualisation should be expanded.

Provide Strategic advice and guidance:

This capability will depend on the level of Engineers appointed in the SOC. This service could also be seen as complementary to the overall SOC service.

Forensic and Investigative functionality:

Most often offered by a team outside the SOC. This might not be a core function of a SOC. A SOC should have the capability to support the forensic process, but not necessarily as a core function.

Vulnerability Management:

The question was asked as to what level of vulnerability management service will be provided? MoE's should also be broken down to reflect at least guidance, management, and strategy.

Network and Security Device Management

The reviewer is not convinced that this really is a SOC function. It could happen that calls are logged to 3rd parties. The same applies to internal organisations. Incident management is the area where this happens. The question needs to be asked: "what are the minimum services and functions required to be provided by a SOC?" Anything at the periphery should be viewed as complementary services or functions.

Security Awareness Training:

Also not seen as part of a SOC. We should not overcomplicate services and functions. Functions and services should be kept at a minimum and should be qualitative, with a checklist.

Status Monitoring and Incident Detection:

Service levels and guaranteed commitments by SOCs with respect to reaction should be included as part of the MoE's, for example 10 minutes notification on incident detection.

SOC Business Requirements:

The SOC should not take on too much. The question was raised as to why these aspects were needed. It depends on what you are looking at - customer can have their own SOC, or use a 3rd party, or use a specialist MSSP. Business requirements are not applicable if running an in-house SOC. The business requirements would then be part of the functionality of a bank. These are supporting requirements which could be relevant to MSSP's. We need to try and simplify the model and focus on core functions. The focus should be on functional and service requirements.

Expert Reviewer # 2 Marco Perreira

Mr Perreira works at Hewlett Packard as part of the Security Sales team. Previously, he was the EMEA Security Practice Manager for WIPRO, where he was responsible for developing and delivering security offerings, including SOC services across multiple WIPRO clients. Thus, we believe that he has the experience and expertise to review the proposed solution.

SOCs are typically not functioning properly because there are no proper processes and controls. Change management, release management etc. has to be done according to business requirements. The Zachmann framework or similar should be used for enterprise planning. If organisations or MSSPs are using the entire SOC value chain, then eTOM is a better fit. However, it is very uncommon that the entire value chain is used. The framework is not as applicable to internal SOCs as it is to MSSP's. We need to understand business and how it runs IT by means of a consultative process, and adapt the framework according to business requirements.

It is also extremely important to map business processes to SOC functions. These are not captured in COBIT/ITIL/ISO etc. We need to consider the architectures to map business processes to ITIL/ISO/COBIT.

It is important to define business requirements in order to ensure that business value is derived from the SOC. SOCs need to provide security intelligence.

We need to understand and map business processes back to the framework. These elements need to be captured in the model. We should also consider TOGAF to do the alignment to the business objectives.

TOGAF is a key component that is missing. Using TOGAF will ensure that the framework is developed correctly the first time.

The following functions and services should also be included, since these are key to next-generation SOCs: Configuration Management, Change Management and Release and Deployment Management.

Next-gen SOCs have other elements that need to be considered, such as mapping between physical security and logs from security devices. These aspects need to be included in the framework. Big data should also be included as part of the functionality of SOCs. There should be convergence in a next-generation SOC where all aspects of security are controlled, including governance and physical security.

Recommendations:

Event Log Collection:

Aspects to consider are how to ensure that a SOC receives the correct logs, and also how to ensure that the correct logs are sent to the SIEM. We furthermore have to ensure that the logs contain the correct information needed from a business or compliance perspective. SOCs cannot collect absolutely everything. Architecture design should be used to determine business requirements, thus enabling SOCs to determine what is needed from a log perspective. We need to think from a business perspective, and not only from an IT perspective.

Event Log Management

Business mapping or alignment should be included as part of the MoE's

Incident Management

The entire incident management lifecycle should be represented and must be illustrated here. Incidents should be transferred to a War room, or some other Cyber incident response capability. This is one of the absolute key differentiators when considering SOC maturity. This is the definitive function of a SOC and should be expanded. It should constitute almost 50% of the SOC score.

Reporting and visualisation

This function should be aligned to the business. Reports and the visualisation of security should enable evaluation, direction and monitoring. How we build the report is important. Reporting and visualisation should be broken up into separate functions with separate MoE's.

Threat Intelligence

Threat feeds are in most cases present, but are not used properly, or are mostly just used for show/customer visits. Threat sources should be there, but it should be determined how much value you get from them, and how you would prove the value you get form them from a validation perspective.

Forensic and Investigative functionality

This aspect is all about incident and breach management It includes how well you respond to an incident; forensic readiness will assist with this. This function also assists with protecting the chain of custody and evidence. If not collected properly, it will not have any value in court. This is an extremely important function from a financial institute, government and national SOC perspective. This function forms part of operations management. It is an absolute key component of the framework.

Vulnerability Management

The values of assets need to be understood. Asset values and criticality needs to be captured, so that a proper review and mapping against vulnerabilities can be done.

Business Impact Analysis

Asset CIA ratings should include this - event logs need to be collected, and assets must be mapped to business objectives in order to measure effectiveness.

Security Awareness Training

This should be part of the organisational function. Awareness is a key factor. Could be part of the SOC, but should be everywhere all the time. Will more likely be part of SOC as a service function, and not in a different capacity.

Problem Correction

This should be renamed to breach management. Problem management might fall under incident management.

Security Systems and Software (management of security technical controls)

There is no consensus on this. The SOC is the center or heart of everything that is technical. This function will only be as successful as governance and alignment to business. Some people think all security devices should be managed from a SOC. The SOCs focus is on event management. Considering the broad function of SOCs, this should be a critical function. Most people do not see the SOC as doing more than event management.

Threat and vulnerability research and investigation

This serves as a key differentiator.

SOC Business Requirements

This is not a main differentiator. These are the basics that are needed to sell and market SOCs. This is a support function, and will not contribute to the success of a SOC on functional aspects.