Classification of Security Operation Centers

Pierre Jacobs, Alapan Arnab, Barry Irwin
Department of Computer Science
Rhodes University
Grahamstown, South Africa
pjacobs@csir.co.za, alapan@gmail.com, b.irwin@ru.ac.za

Abstract — **Security Operation Centers (SOCs) are a necessary service for organisations that want to address compliance and threat management. While there are frameworks in existence that addresses the technology aspects of these services, a holistic framework addressing processes, staffing and technology currently do not exist. Additionally, it would be useful for organizations and constituents considering building, buying or selling these services to measure the effectiveness and maturity of the provided services. In this paper, we propose a classification and rating scheme for SOC services, evaluating both the capabilities and the maturity of the services offered.**

Keywords- Security Operations Center; Computer Incident Response Team, maturity model; classification matrix

I. INTRODUCTION

A Security Operations Centre (SOC) can be defined as a centralized security organization that assists companies with identifying, managing and remediating distributed security attacks [1]. Depending on the capabilities required from a SOC by the enterprise or client, a SOC can also be responsible for the management of technical controls. The end-goal of a SOC is to improve the security posture of an organization by detecting and responding to threats and attacks before they have an impact on the business.

SOCs can either be implemented internally by an enterprise, or can be purchased as a service from security service providers, and both approaches have their advantages and disadvantages. Currently, there are no objective mechanisms to determine the maturity level of the processes and service offerings within the SOCs. Furthermore, geographically dispersed SOC's from the same organization can differ in maturity and capability, and there is currently no objective means to measure the disparity.

The main functions of SOC's are to monitor security events from deployed security technical controls as well as other critical assets, and respond to those events [2]. This allows for SOC service consumers to have situational awareness, reduces risk and downtime, and assist with threat control prevention [3].Other tasks could also be allocated to the SOC, such as management of security controls, awareness campaigns, and availability monitoring of the controls and assets.

Additionally, a SOC can also aid with compliance management through the monitoring of events against specified compliance objectives, such as providing audit log retention requirements and monitoring the effectiveness of implemented technical controls.

As opposed to a SOC providing Security Operations services – including incident management, a Computer Security Incident Response Team (CSIRT) provides two basic services [4]. These are Incident response, and proactive measures to prevent network incidents. In most CSIRTs, proactive measures are not necessarily required [4]. Thus, CSIRTs can be considered to be specialized SOC offerings.

Although there are numerous frameworks for technologies used in SOCs (such as [5] [6] and [1]), there is no holistic framework addressing processes, staffing and technology aspects of a SOC. Furthermore, there is no maturity model that can be used to evaluate the effectiveness and capabilities of a SOC.

In this paper, we present a model to measure the effectiveness and capabilities of a SOC, through three aspects:

- The Aspects of SOC services
- The Capability of the SOC aspects.
- The Maturity of SOC processes per aspect

Maturity models or frameworks implies perfect or explicitly defined, managed, measured and controlled systems [7] and [8]. 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 SOC's or CSIRT's, or choosing a vendor providing those services. This paper does not aim to define the exhaustive functional aspects of a SOC, but rather define the critical aspects, and this model can be expanded upon with further functional aspects.

This paper is organized as follows – in Chapter II, we review existing, industry accepted maturity models and discuss existing SOC capability and maturity models. This is followed by our proposed SOC classification model in Chapter III. Chapter IV summarises the intended future work before concluding in Chapter V.

II. RELATED WORK

Currently no proper classification scheme or matrix exists when discussing SOC's. We have therefore based our classification model on industry accepted models, specifically for maturity models as well as expected services and capabilities for Security Operations.

A. *Industry accepted maturity models*

When describing the maturity level of a SOC, it would be prudent to use existing established Information Technology (IT) management framework such as Control Objectives for Information Technology (CoBIT) and Information Technology Information Library (ITIL), coupled with information security frameworks such as ISO/IEC 27001. The CoBIT framework covers all aspects of IT in the business, and is supported by ITIL, which covers effectiveness and efficiency of operations. The Figure 1 depicts the relationship between different standards and frameworks:

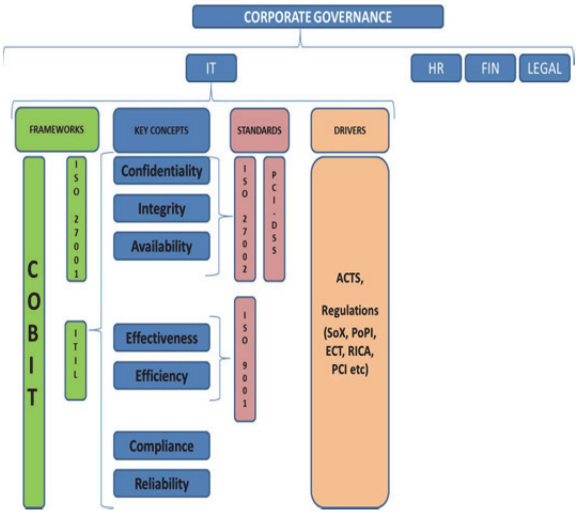


Figure 1: Relationship between Standards, Frameworks and their drivers

In order to have a repeatable model, SOC's will have to be classified for each aspect (the solutions offered by the SOC), the capability (how much functionality is offered), and the maturity (how well the SOC can deliver the functionality).

CoBIT identifies five maturity levels for management and control of IT processes, which allows for benchmarking and identification of capability improvements. This approach was derived from the Software Engineering Institute (SEI) [9].

The five CoBIT maturity levels 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 also not something which can be measured with 100% accuracy, since some implementations will be in place at different levels. These levels will however assist in creating a profile.

The ITIL Process Maturity Framework (PMF) also identifies five Process Maturity Levels [10], and as illustrated in Figure 1, ITIL focus 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 are:

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

According to Wim Van Grembergen *et al* [11], *"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) focusses on Organizations software processes, and the evaluation of the capability of these processes [12][13].

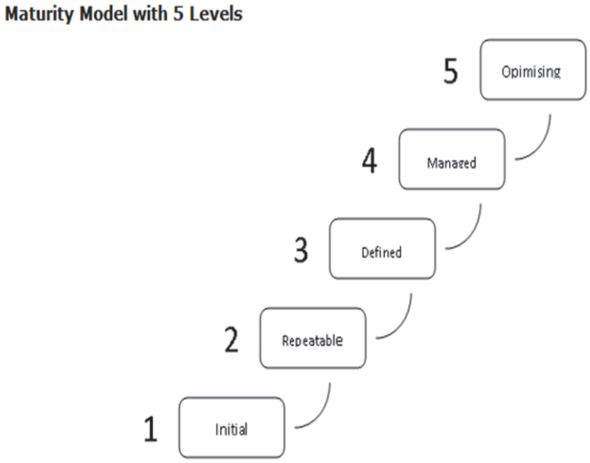


Figure 2: The Software Capability Maturity Model [12]

The National Institute of Standards and Technology (NIST) [14] uses five security maturity levels. These are:

- IT Security Maturity Level 1: Policies
- IT Security Maturity Level 2: Procedures
- IT Security Maturity Level 3: Implementation
- IT Security Maturity Level 4: Test
- 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) [15]. The five capability levels are:

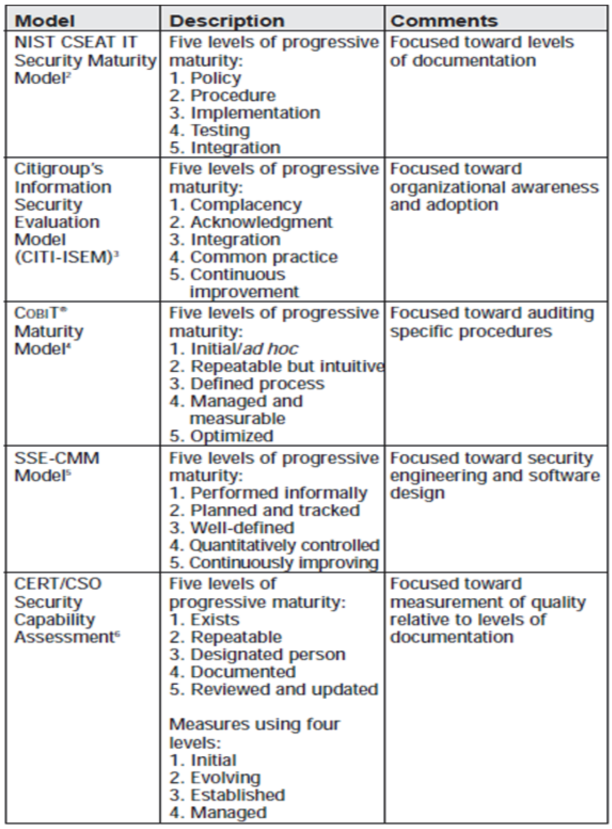
- Level 1 – Base practices are performed informally

- Level 2 – Base practices are planned and tracked
- Level 3 – Base practices are well defined
- Level 4 – Base practices are quantitatively controlled
- Level 5 – Base practices are continuously improving

A systematic approach to measuring the maturity of a security technical or administrative control should [15]:

- Generate reproducible and justifiable measurements of the security posture and service to organization or client,
- Measure something of value to the client or organization,
- Determine progress in security posture and service delivery to clients,

Assist in determining the order in which security controls should be applied as well as the resources needed to apply the security program.



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

Table 1: Published Security Maturity Models[16]

The CERT/CSO Security Capability Assessment model consist of five maturity levels [17]. These are aimed at the quality of documentation. The levels are:

- Level 1 – Exists
- Level 2 – Repeatable
- Level 3 – Assigned Responsibility
- Level 4 – Documented
- Level 5 – Revised and Updated

Table 1 summarizes the published Security Maturity Models and their focus [16]. The derived proposed SOC Process Maturity model is summarized in Table 2.

The six step model 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.

B. *Aspects of a SOC*

SOC's provides situational awareness for Organisations on their security posture, reduces risk and downtime, prevents and controls threats, ease administrative overhead, serves as an escalation path and assists with audit and compliance [3]. In other words, a SOC prevents, detects, reacts, recover from security related incidents, and in the process assists with compliance.

A SOC receives events from different implemented technology solutions, both agentless or with an agent, and the technologies could be implemented locally or across a geographically dispersed environment.

SOC aspects are numerous, and should constantly be updated. Aspects describe the functionalities of a SOC, and capabilities describe how well it performs these functions [18] and [2].To be able to compare different SOCs, it is important to define aspects against which they can be measured. Aspects can be grouped into primary and secondary aspects. Primary aspects are those aspects which will be found in any SOC, and is defining of the main functionality of a SOC. These would be the minimum functions and aspects an entity should have to be classified as a SOC. Secondary are those offered over and above SOC normal functions

We have derived the following primary aspects through a combination of a number of security management and control frameworks [19], [20] [6] [21] and [22], including ISO 27000 series and SANS Crititcal Controls [2] and [23] .

- Log Collection

  Refers to a centralized collection to security, system and transactional activity logs. A service with low capability in log collection, will provide a best effort service, with no guarantee in collection; while a service with high capability in log collection, will provide a collection guarantee of over 99% of produced log events.

- Log Retention and Archival

  If a log file contains useful and relevant information which can be used in future, it must be retained. Acts and legal requirements can also demand that logs be retained. A service with low capability will store logs for a limited time and have size constraints, and storage will not be forensically secure. A high capability service will store logs with minimal time or size constraints, and comply with customer and legal requirements such as guaranteed recovery and non-repudiation.

- Log Analysis

  Refers to the capability of the SOC to analyse raw data and present the result as usable, actionable and understandable information and metrics. A low capability service will be able to present only raw data and logs from a limited amount and type of devices in limited formats, and a high capability service will be able to provide metrics and dashboards from a wide range of formats and type of devices.

- Monitoring of Security Environments for Security Events.

  According to the ITIL glossary and abbreviations of 2011 [24], monitoring is *"Repeated observation of a configuration item, IT service or process to detect events and to ensure that the current status is known."* A Service with a low capability will provide basic monitoring during office hours with no guaranteed response levels in place. A highly capable monitoring service will provide guaranteed services on a 24x7 follow the sun principle and can prove improvement in security posture.

- Diversity of devices integrated

  Refers to the type of devices and vendors which can be integrated and managed from the SOC. It also includes concepts such as available skillsets within the SOC. A Low capability service will be able to monitor limited device types from limited vendors, and also have a limited capability to understand and interpret the vulnerabilities against those device types. A Highly capable service will experience little or no restrictions on the type of devices and vendors to monitor, and will have the expertise to understand vulnerabilities and threats seen against those devices.

- Event Correlation and Workflow.

  This refers to the capability to correlate events between different device types and vendors, as well as kick off workflows in response to correlation rules being triggered. Correlation rules could be basic, to AI based automated rules. Services with a low capability supplies only basic, manual correlation rules with no workflow capability. A highly capable service will provide complex, automated correlation rules integrated into enterprise wide workflow systems.

- Incident Management

  This refers to the ability to react to, and escalate incidents. A Service with a low capability will manually create and react to incidents. Escalation is also manual. A highly capable service will have Incident Management and escalation automated, and tracked and managed by integration into enterprise wide incident management systems.

- Reaction to threats.

  This could be both real-time, as well as potential threats and vulnerabilities which need to be escalated and corrective pro-active measures taken to mitigate. The latter will not necessarily be classified as incidents. This is as opposed to reactive behavior to mitigate virus outbreaks or attacks in progress which is already an incident. Low capability services will have no in-house research and external threat feed capability, and a highly capable service will have a research contingent with automated, subscribed threat and vulnerability feeds from multiple external providers.

- Threat Identification

  Refers to the capability of a SOC to identify threats and vulnerabilities either in real time and as part of a research capability. A low capability service will have limited threat identification capabilities, while a highly capable service will have a research capability, as well as real time querying of integrated 3rd party threat management systems.

- Reporting

  This refers to the capability of providing security related reports to clients. A Service with a low capability will provide out of the box reports in limited format and platforms, whereas a highly capable service provides on-demand, ad-hoc, analysed reports to clients in different formats and via different platforms.

Secondary aspects are functions which are offered over and above the primary SOC services. Secondary services include, but is not limited to:

- Malware analysis
- Vulnerability Scanning
- Vulnerability Analysis
- Device Management
- Identity Attestation and Recertification
- Penetration testing
- Type of Industry verticals monitored. Threats against a Financial Institution's network will differ from those against a Supervisory Control and Data Acquisition (SCADA) network.
- Integration with Physical Security controls.

The secondary aspects are not exhaustive and are expected to change over time. Furthermore, secondary aspects could also be industry or geographic specific.

These aspects will be further defined by their capabilities and maturity.

III. Model for SOC Maturity and Capability

Based on maturity models discussed previously, we propose a 6 step maturity model, which we have aligned to the models discussed previously.

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)

Table 2: Process Maturity

The cube in Figure 4 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 [25].

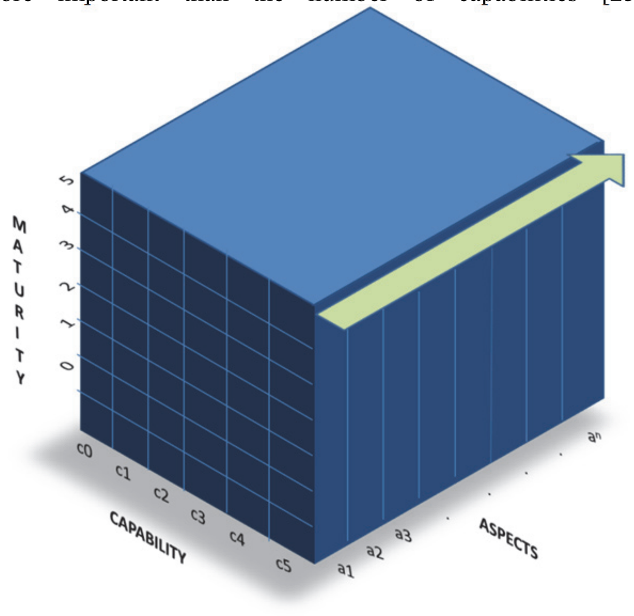


Figure 4: SOC Classification Cube

The Maturity, Aspects and Capability of SOCs can be 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 aspect scores, where each aspect is scored on Capability and Maturity expressed as a score out of 100.

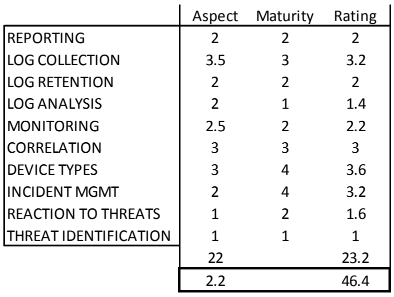
$\alpha = 0.4$

$\beta = 0.6$

This will provide a weighting which 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 aspects higher than others.

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

We have used the above approach, and applied it to rate a known SOC provider in South Africa, which we are well acquainted with. The breakdown of the individual aspects as shown in Figure 5, and the total score of the SOC is 46.4. While this particular SOC service has some strong services, the majority of the services are below par, and this is reflected in the overall score. As discussed in Section IV, we intend to extend this rating formally across multiple providers in South Africa , which would allow us to build a comprehensive analysis of the SOC services market in South Africa, including the strengths and weaknesses of various players together with the overall industry norms.



	Aspect	Maturity	Rating
REPORTING	2	2	2
LOG COLLECTION	3.5	3	3.2
LOG RETENTION	2	2	2
LOG ANALYSIS	2	1	1.4
MONITORING	2.5	2	2.2
CORRELATION	3	3	3
DEVICE TYPES	3	4	3.6
INCIDENT MGMT	2	4	3.2
REACTION TO THREATS	1	2	1.6
THREAT IDENTIFICATION	1	1	1
	22		23.2
	2.2		46.4

Table 3: SA MSSP Rating

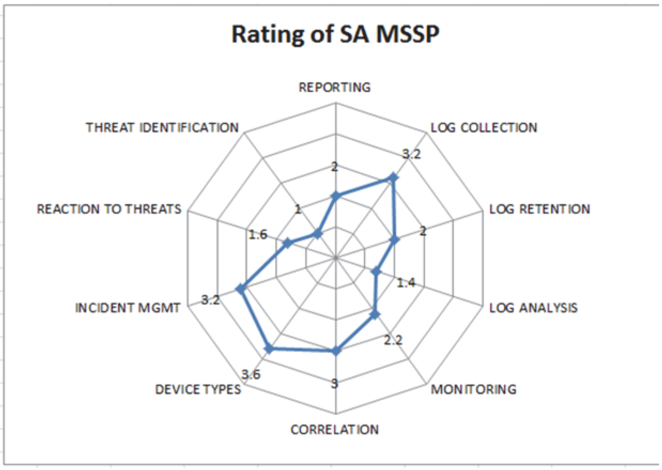


Figure 5: Rating of SA MSSP

IV. Future Work

We plan to verify the completeness of the model, through engagement with both consumers and providers of SOC services, and to thereafter classify existing providers in the South African environment to understand the current strengths, and weaknesses, as an additional verification for the model.

V. Conclusion

After having done extensive research and literature reviews, no literature or references could be found on an Industry accepted framework or comprehensive classification scheme for SOCs.

Using this proposed classification matrix, it is possible to assign a weighting to SOC capability and maturity levels. This can assist SOC owners in determining their status, as well as identify where growth and improvement is needed. Customers looking at making use of SOC services can use this model to determine the level of service they can expect, as well as to allow them to make an informed decision when signing up for SOC services.

Acknowledgment

We would like to thank Schalk Peach and Karel Rode for their early review and feedback on the proposed model.

References

[1] Afsaneh Madani et al, “Log Management comprehensive architecture in Security Operation Center(SOC),” *2011 International Conference on Computational Aspects of Social Networks (CASoN)*, 2011. [Online]. Available: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6085959&tag=1.

[2] Kevin Warda, “A Fundamental and Essential look into Managed Security Services,” *SANS (GSEC) Practical Assignment Version 1.4c – Option 1 March 28, 2005*, 2005. [Online]. Available: http://www.giac.org/paper/gsec/4432/fundamental-essential-managed-security-services/107412.

[3] Diana Kelley and Ron Moritz, “Best Practices for Building a Security Operations Center,” *The (ISC)2 Information Systems Security*, 2006. [Online]. Available: http://www.infosectoday.com/Trial/Kelley.pdf.

[4] C. Thompson, “Incident Response and Creating the CSIRT in Corporate America,” *SANS Institute InfoSec Reading Room*, 2001. [Online]. Available: http://www.sans.org/reading_room/whitepapers/incident/incident-response-creating-csirt-corporate-america_642.

[5] Renaud Bidou, “Security Operation Center Concepts & Implementation,” 2004. [Online]. Available: http://academic.research.microsoft.com/Publication/12790770/security-operation-center-concepts-&-implementation.

[6] Diana Kelley and Ron Moritz, “Best Practices for Building a Security Operations Center,” *Information Security Journal: A Global Perspective*, 2006. [Online]. Available: http://www.infosectoday.com/Trial/Kelley.pdf.

[7] S. P. M. Ibrahim Al-Mayahi, “ISO 27001 Gap Analysis - Case Study,” 2012. [Online]. Available: http://elrond.informatik.tu-freiberg.de/papers/WorldComp2012/SAM9779.pdf.

[8] Andrea Pederiva, “The COBIT Maturity Model in a Vendor Evaluation Case,” *Information Systems Control. Journal*, 2003. [Online]. Available: http://www.isaca.org/Journal/Past-Issues/2003/Volume-3/Documents/jpdf033-COBITMaturityModel.pdf.

[9] Mark Adler et al, “CobiT 4.1 Framework,” 2007. [Online]. Available: http://www.isaca.org/Knowledge-Center/cobit/Documents/CobiT_4.1.pdf.

[10] Ian MacDonald, “ITIL Process Assessment Framework,” 2010. [Online]. Available:

http://www.itsmfi.org/files/ITIL Process Assessment Framework - MacDonald.pdf.

[11] Wim Van Grembergen and Steven De Haes, “Measuring and Improving IT Governance Through the Balanced Scorecard,” *Information Systems Control Journal*, 2005. [Online]. Available: http://www.isaca.org/Journal/Past-Issues/2005/Volume-2/Documents/jpdf052-measuring-and-improving.pdf.

[12] Bill Curtis et al, “Software Capability Maturity Model (CMM).” [Online]. Available: http://www.itgovernance.co.uk/capability-maturity-model.aspx.

[13] IT Governance, “Software Capability Maturity Model (CMM).” [Online]. Available: http://www.itgovernance.co.uk/capability-maturity-model.aspx.

[14] NIST, “Security Maturity Levels,” 2012. [Online]. Available: http://csrc.nist.gov/groups/SMA/prisma/security_maturity_levels.html.

[15] Mike Phillips, “Using a Capability Maturity Model to Derive Security Requirements,” 2003. [Online]. Available: http://www.sans.org/reading_room/whitepapers/bestprac/capability-maturity-model-derive-security-requirements_1005.

[16] Steven Akridge and David A.Chapin, “How Can Security Be Measured?,” *Information Systems Audit and Control Association.*, 2005. [Online]. Available: http://www.isaca.org/Journal/Past-Issues/2005/Volume-2/Pages/How-Can-Security-Be-Measured.aspx.

[17] M. Sajko, “Measuring and Evaluating the Effectiveness of Information S ecurity,” 2007. [Online]. Available: http//www.academypublish.org/papers/pdf/310.pdfw.academypublish.org/papers/pdf/310.pdf.

[18] Reply Communication Valley, “SECURITY OPERATION CENTER.” [Online]. Available: http://www.reply.eu/1937_img_COMVR11_SOC_eng

[19] D. Del Vecchio, “The Security Services a SOC should provide,” 2012. [Online]. Available: http://www.socstartup.blogspot.it/2012/09/the-security-services-of-soc.html.

[20] Cisco Systems, “How to Build Security Operations Center (SOC),” 2007. [Online]. Available: ftp://ftp-eng.cisco.com/cons/workshops/SP-Powersession-Thailand-Jan-2007/SPSEC-610-Security-Operations-Centers-Basics-Version-2.pdf.

[21] Michael Protz et al, “A SAS® Framework for Network Security Intelligence,” 2009. [Online]. Available: http://www2.sas.com/proceedings/sugi30/190-30.pdf.

[22] Cisco Systems, “Cracking the Code for a SOC Blueprint Architecture, Requirements, Methods and Processes and Deliverables,” *Cisco Networkers*, 2006. [Online]. Available: ftp://152.33.34.12/CiscoLive/IT Insight/BRKITI-1012.pdf.

[23] ISO / IEC, “ISO/IEC 27001:2005 Information technology -- Security techniques -- Information security management systems -- Requirements,” 2005. [Online]. Available: http://www.gov.mu/portal/goc/women/file/AnnexIX1302.pdf.

[24] Ashley Hanna, “ITIL® glossary and abbreviations,” 2011. [Online]. Available: http://www.itil-officialsite.com/nmsruntime/saveasdialog.aspx?lid=1180&.

[25] K. Chung, “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*, 2006. [Online]. Available: https://www.isc2.org/PressReleaseDetails.aspx?id=2714.