Framework for the implementation of business cybersecurity capabilities

P.C. Jacobs[1,2], Prof. S.H. von Solms[2], Prof. M.M. Grobler[1,2]
[1] Council for Scientific and Industrial Research, Pretoria, South Africa, [2] University of Johannesburg, Johannesburg, South Africa

Keywords: Cybersecurity; capability framework; cybersecurity structures

Towards a framework for the development of business cybersecurity capabilities

Information and Communications Technology is often seen as a critical organisational asset. To prevent loss of revenue and money, as well as to protect organisational reputation, this asset must be protected from threats and vulnerabilities. Organisations use different standards, frameworks and best practices when addressing cybersecurity. These governance documents could be chosen based on legislative or corporate governance requirements, and are most often industry specific. These documents typically prescribe sets of controls to be implemented, such as technical controls, administrative controls and physical controls. Most of these documents also describe very specific capabilities that a business has to develop in securing their cyberdomain. Capabilities, consisting of people, processes and technology, are meant to achieve outcomes or effects, and are applicable to the operational domain. Initial research has shown that no cybersecurity capability development framework applicable to the business domain exists. In this article, a framework called the Business Cybersecurity Capability Development Framework (BCCapDev framework) is proposed. In developing the BCCapDev, a modular approach is followed, starting with the identification of requirements for such a framework. Input into the BCCapDev framework such as legal requirements and business governance requirements are identified. Existing standards, frameworks and best practices are consulted, and capabilities identified, as well as actors and stakeholders. Mechanisms to align BCCapDev processes with business are identified, as well as a methodology to build the capability. The framework is developed in such a way that it is modular, reusable, and independent to changes in standards, frameworks or best practices. The BCCapDev is also developed flexible enough to be industry neutral.

1. Introduction

Threats to the internet are increasing in volume, complexity and velocity, and globally governments have lost in excess of $125 billion due to cybercrime (NATO Cooperative Cyber Defence Centre of Excellence 2012). Already in 2014 Wolfpack Information Risk has stated that cybercrime is costing South Africa R5.8 billion per annum (C. Fripp 2014), and that more than 70% of South Africans have been victims to cybercrime (Live 2013). The instances of industrial espionage and foreign economic collection, both in South Africa and globally, is on the rise too partly due to the anonymity offered by the internet (NATO Cooperative Cyber Defence Centre of Excellence 2012) and the global integration of ICT (S. Mukwevho 2015). The FBI in 2012 investigated economic espionage cases responsible for losses to the US economy to the value of $13 billion (NATO Cooperative Cyber Defence Centre of Excellence 2012). At the same time, the integrity and resilience of critical infrastructure is also threatened by means of unauthorised access, destruction of resources and manipulation of data and networks. The rise of malware such as Duqu, Stuxnet and Flame is a cause for concern since these worms are used to establish control over remote systems (NATO Cooperative Cyber Defence Centre of Excellence 2012).

The World Economic Forum (WEF), in their "The Global Risks 2015 report" warned that 90% of businesses globally are not adequately prepared to protect themselves against cyberattacks (World Economic Forum 2015). Not preparing for cyberattack could expose businesses to loss of revenue, reputational loss, disrupted operations and regulatory action (D. Gabel; B. Liard & D. Orzechowski 2015). To improve their cybersecurity postures, businesses could consider different cybersecurity frameworks, standards and best practices. Some of these are the National Institute of Standards and Technology (NIST) Cybersecurity Framework (NIST 2014b), the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), ISO/IEC 27001:2005 (ISO/IEC 2005). Business also has to consider normative documents such as standards, and authoritative documents such as international and national acts and regulations. The frameworks, normative documents, best practices and authoritative documents give rise to the requirement for specific cybersecurity capabilities.

At the time of writing, no framework for the development of cybersecurity capabilities for business could be found as part of a literature search. The Association for Computing Machinery (ACM) (ACM 2016) CiteSeer^{x} (CiteSeerX 2016), Google Scholar (Google 2016), Institute of Electrical and Electronics Engineers (IEEE) (IEEE 2016) and Microsoft Academic Research (Microsoft 2016) were consulted – all being strong sources of literature in this area - and no cybersecurity capability development frameworks could be found.

2. What is a capability

BusinessDictionary.com defines a capability as the "measure of the ability of an entity (department, organization, person, system) to achieve its objectives, especially in relation to its overall mission", (BusinessDictionary.com 2016) while Ulrich and McWhorter defines a business capability as "what a business does at its core". A business capability does not describe how or where things are done (W. Ulrich & W. McWhorter 2010). Dickenson and Mavris defines a capability as "… the ability to achieve a desired effect under specified standards and conditions through combinations of ways and means to perform a set of tasks" and also "… the ability to execute a specified course of action that is defined by a user, and is expressed in non-equipment based operational terms" (C. Dickerson and D. N. Mavris 2010). As can be seen from these definitions, capabilities are meant to achieve outcomes or effects, and are applicable to the operational domain.

Capabilities have the following characteristics (W. Ulrich & W. McWhorter 2010). A capability:

- describes "what" is being done (It does not describe how something is done, a process describes the "how").
- has a specific outcome.
- is clearly defined.
- the intent of a capability is unique.
- provides solutions, and are framed by its parent capabilities.
- is unique and require and use unique information.
- is a pure business view of the business.
- are framed roles, and resources having those capabilities.

Capabilities describe what something must do, and its supporting processes describes how something is done (C. Dickerson and D. N. Mavris 2010). A capability is a combination of processes, knowledge, skills and behaviours (people), tools and systems (technology) and an organization (Strategy& 2012).

3. BCCapDev Framework Development

The purpose of the BCCapDev framework is to provide businesse with a comprehensive, yet flexible framework to assist with the identification of cybersecurity capabilities, and the implementation thereof. The aim is to improve the security posture of business by identifying and deploying cybersecurity capabilities.

The BCCapDev framework consists of six levels in order to cater for the various levels of governance and the wide range of stakeholders involved in BCCapDev framework. At each level of the framework the following three questions are asked:

- What is needed? – this is the requirements identified section.

- Why is it needed? – these are the driving factors necessitating each level. This is expressed in the written section of each specific level.
- Who is responsible for it? – these are the actors and stakeholders

In the developing of the capabilities themselves and also the identification of processes, a fourth question is asked. This question relates to how the capability is developed and implemented, and how its processes are identified.

- How will it be done? – these are the processes supporting the development of the capabilities such as enterprise architecture and systems engineering.

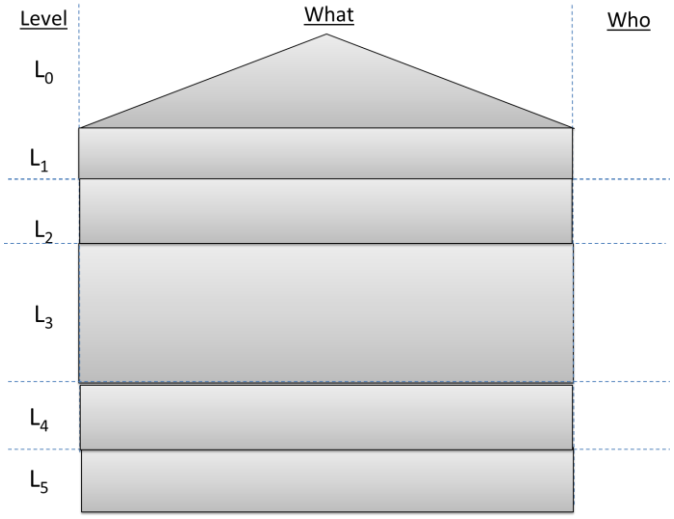

Figure 1: BCCapDev High-Level Framework

The BCCapDev Framework application is illustrated in terms of a South African context.

3.1 BCCapDev Framework Level 0

Level 0 describes all normative and authoritative documents such as laws, organisational policy and strategy and adopted standards. This is needed to comply with national and international laws, and furtherance of organisational strategy and policy. Government is responsible for laws and government or industry appointed bodies are responsible for the determination of regulatory requirements. From a business perspective, the board of directors is responsible for the development of their business strategy (K.B. Jensen 1992). Policy development could be delegated to employees, and even third party service providers. Different models for developing strategy exists, and businesses should choose the model best suited to them, and adapt it to their needs (C. McNamara 2016).

From a South African context acts such as the Protection of Personal Information Act (South African Government 2013), and the draft South African Cybercrimes and Cybersecurity Bill (Minister of Justice and Correctional Services 2015) serves as

examples of authoritative documents, while the decision to use the ISO/IEC 27001:2005 (ISO/IEC 2005) as an information security standard serve as an example of a normative document. Depending on the type of business and the industry it does business in, regulatory bodies could be appointed, such as the Internet Service Providers' Association (ISPA) (ISPA 2016) serving as a regulatory body for internet service providers in South Africa. Level 0 of the BCCapDev Framework is displayed in Figure 2.

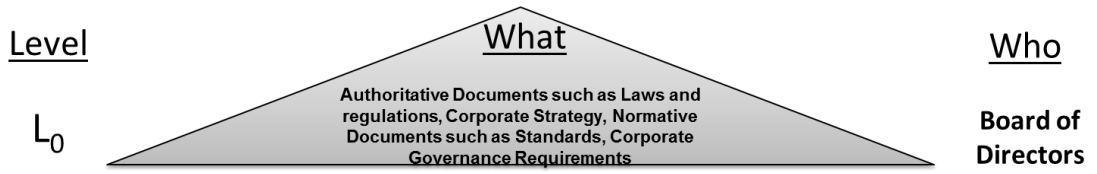

Figure 2: BCCapDev Framework Level 0

3.2 BCCapDev Framework Level 1

Level 1 describes the need for an overall controlling body to facilitate the planning and implementation of the cybersecurity capabilities. The appointment of a controlling body ensures accountability and leadership during the implementation phase. The controlling body uses normative and authoritative documents as developed in Level 0 as input in the determination of organisational cybersecurity capabilities. Most frameworks, standards and best practices prescribe a risk based approach in the determination of cyberthreats and cyberrisks (ISO/IEC 2005), (R.S. Ross 2014), (Adler 2007).

It is the experience of the authors that the identification of these threats and risks is paramount in the determination of applicable cybersecurity capabilities, and the prioritisation of the development of these capabilities. Organisations can choose from different risk management standards to use as normative documents, such as ISO/IEC 31000:2009 Risk management -- Principles and guidelines for a generic organisational approach (ISO/IEC 2009), or ISO/IEC 27005:2011 Information security risk management for an information security specific approach (ISO/IEC 2011). Industry specific risk management standards also exists, such as ISO/IEC 27011:2008 Information security management guidelines for telecommunications organizations based on ISO/IEC 27002 (ISO/IEC 2008) and ITU-T X.1055 Risk management and risk profile guidelines for telecommunication organizations (ITU-T 2008) – specifically aimed at telecommunications businesses.

The cybersecurity risk management function is a capability in its own and is described by various standards and frameworks such as NIST (Furlani 2011) , The European Union Agency for Network and Information Security (ENISA) (ENISA 2016), Information Systems Audit and Control Association (ISACA) (ISACA 2016) (Adler 2007), System Administration, Networking, and Security Institute (SANS) (J. Wurzler 2013), and ISO/IEC 27001:2005 (ISO/IEC 2005). The authors have placed the cybersecurity risk management capability at a higher level than the capabilities which is discussed in Section 3.4. This is because the output of the cybersecurity risk

management process serves as input into the determination of the business cybersecurity capabilities, and is a capability that needs to be initiated and managed by the overall controlling body.

The overall controlling body is also responsible for developing and defining the capability operational model. An applicable and scalable model should be identified and implemented such as the plan-build-run-monitor model described in the Control Objectives for Information Technology (CoBIT) (Adler 2007), (Weinberg et al. 2013). The role of the overall controlling body can be filled by the Chief Information Officer (CIO), the Information Security Officer (ISO), or the Chief Information Security Officer (CISO). Level 1 of the BCCapDev Framework is shown in Figure 3.

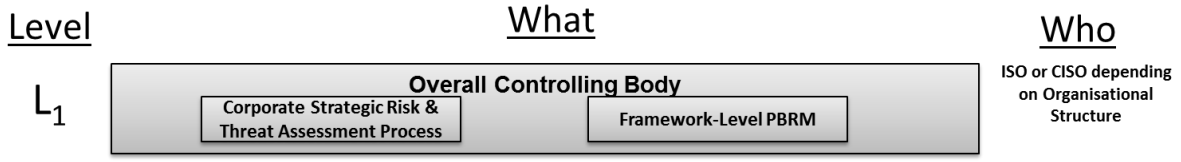

Figure 3: BCCapDev Framework Level 1

3.3 BCCapDev Framework Level 2

The second level of the BCCapDev framework describes the organisational structure of the business. This is important to identify the different organisational structures, since different normative and authoritative requirements could be applicable to different structures. From a South African perspective, and as an example of an authoritative requirement, all financial and audit statements is required to be kept for a period of seven years as stipulated in the Companies Act, No 71 of 2008 (South African Government 2008). This requirement is applicable to the business's financial function. This requirement directly influences the organisational "recovery" capability which is described in Section 3.4. Act No. 4 of 2013: Protection of Personal Information Act, 2013 (South African Government 2013) is an authoritative document applicable mostly to the human resources organisational function – but not exclusively. Organisational Information and Communications Technology (ICT) could have ISO/IEC 27001:2005 (ISO/IEC 2005) applicable as a normative requirement. Depending on the size and the geographical location of the business, other countries acts and regulations could be applicable. Level 2 serves as a placeholder to be populated with organisational function specific normative and authoritative requirements, and is the responsibility of the internal governance and compliance function. Level 2 of the BCCapDev Framework is shown in Figure 4.

Figure 4: BCCapDev Framework Level 2

3.4 BCCapDev Framework Level 3

In Level 3 of the framework, the capabilities are determined. In its framework for improving critical infrastructure cybersecurity (NIST 2014b), NIST uses the following functions to group cybersecurity categories, sub-categories and informative references:

- Identify
- Protect
- Detect
- Respond
- Recover

For the identification of capabilities, the NIST categories are used. NIST has mapped the categories in its cybersecurity framework core (NIST 2014a) to the major standards and frameworks such as CoBIT (Adler 2007), ISO/IEC 27001:2005 (ISO/IEC 2005) and the SANS critical controls (SANS Institute 2013). The authors utilised the NIST cybersecurity framework core to determine business cybersecurity capabilities, and the completeness thereof was confirmed through the mapping against CoBIT (Adler 2007), SANS (SANS Institute 2013) and ISO/IEC 27001:2005 (ISO/IEC 2005).

The identified business cybersecurity capabilities identified are:

- Identify
  - Asset Management
  - Business Environment
  - Governance
- Protect
  - Access Control
  - Awareness and Training
  - Data Security
  - Information Protection Processes and Procedures
  - Maintenance
  - Protective Technology
- Detect
  - Anomalies and Events
  - Security Continuous Monitoring
  - Detection Processes
- Respond
  - Response Planning
  - Communications
  - Analysis
  - Mitigation
  - Improvements
- Recover

- Recovery Planning
- Improvements
- Communications

The framework is flexible in that the capabilities can be determined using any other means, such as using the output from a security audit, using input from normative and authoritative requirements, and any other framework or standard applicable to the business. Telecommunications businesses could replace the capabilities with those identified in the Telecommunications Forum's (TMForum) enhanced Telecom Operation Map (eTOM) business process framework (TMForum 2013). Technical cybersecurity capabilities could be replaced or augmented with the requirements as expressed in the International Telecommunication Union's Standardization Sector (ITU-T) recommendation X.805 : Security architecture for systems providing end-to-end communications (ITU-T 2004). Businesses in the financial sector could replace or augment the requirements with the Payment Card Industry Data Security Standard (PCI DSS) (PCI Security Standards Council 2010).

In Section 2 the statement was made that a capability consists of people, process and technology components. Development of technical capabilities, or development of technology in support of a capability can be achieved by using Systems Engineering principles (INCOSE 2010). Following this process allows for the determination of user requirements specification (URS), functional and technical specifications, measures of effectiveness (MoE's) and measures of performance (MoP's) for the technological capability (INCOSE 2010).

In identifying the processes and procedures for the capability, an enterprise architecture approach using frameworks such as The Open Group Architecture Framework (TOGAF) (The Open Group 2013) or Layered Enterprise Architecture Development (LEAD) (LEADing Practice 2016) could be considered. This approach further allows for the development - and alignment of business and capability processes with each other (TOGAF 2006). The people and skills component could be developed internally by the business itself, using a framework such as NISTs National Initiative for Cybersecurity Education (NICE) (NIST 2013). Depending on the business and operational model followed, these skills could also be provided by an outsourced service provider. Level 3 of the BCCapDev framework is shown in Figure 5.

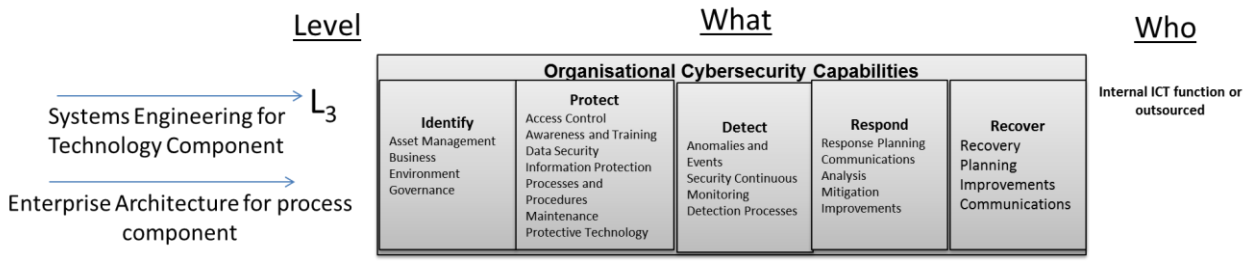

Figure 5: BCCapDev Framework Level 3

3.5 BCCapDev Framework Level 4

Level 4 of the BCCapDev framework describes the structures needed in support of the identified capabilities. To illustrate Level 4, the Respond capability is used. The Respond capability will result in a Security Operations Center system (SOC) (Jacobs P. 2015), a Computer Security Incident Response Team (CSIRT) (ENISA 2015), or a combination of the two. The structures at Level 4 will need its own people and skills, processes and technologies. Systems engineering and enterprise architecture can also be used at this level as discussed in Section 3.4. In the development of the structure, the plan-build-run-monitor models as described in Section 3.1 could be used. Level 4 of the BCCapDev framework is displayed in Figure 6.

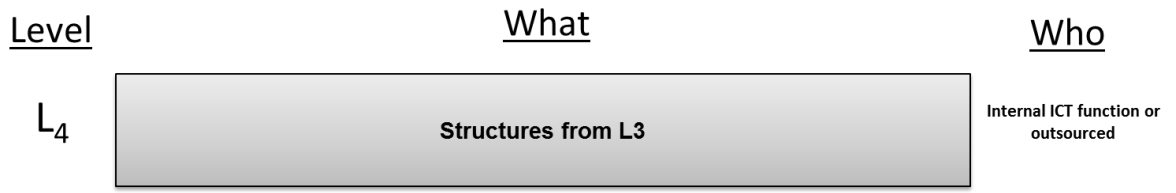

Figure 6: BCCapDev Framework Level 4

3.6 BCCapDev Framework Level 5

Level 5 describes the structure (SOC or CSIRT described in Section 3.5) internal policies, processes and technology specific procedures. These items will govern the operational cycle of the structure. The policies and processes need to be aligned with business, and can be facilitated by an enterprise architecture approach. Level 5 of the BCCapDev framework is displayed in Figure 7.

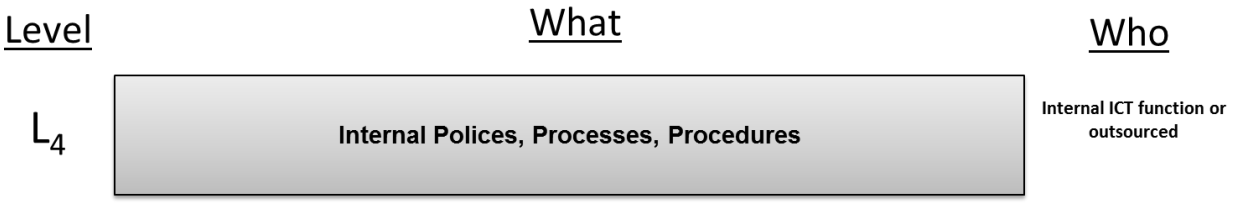

Figure 7: BCCapDev Framework Level 5

3.7 BCCapDev Complete Framework

The complete BCCapDev framework is shown in Figure 8. It illustrates how all levels of the framework is needed for the identification and development of cybersecurity capabilities. The modular nature of the framework is also shown, allowing for the flexibility to change the business's organisational structure to reflect its actual implementation, as well as the fact that the capabilities can be identified from various different sources, and governance requirements applicable to a specific business in a specific sector or industry.

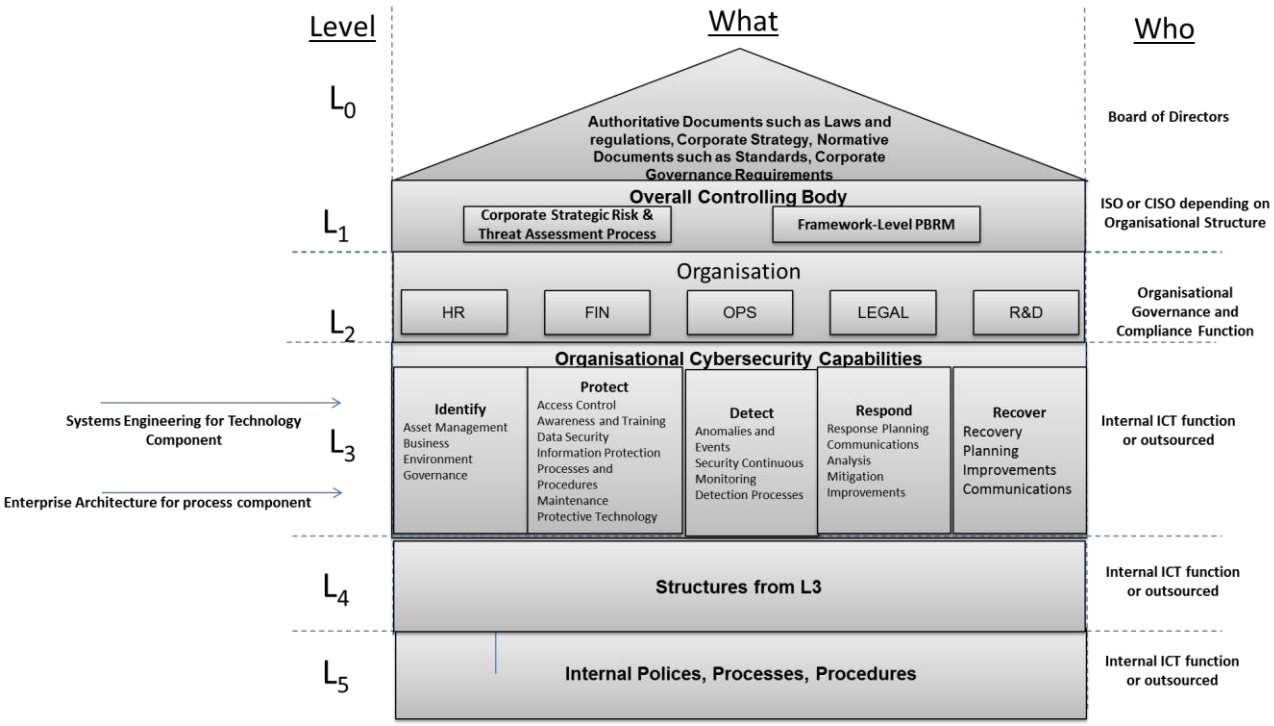

Figure 8: Complete BCCapDev Framework

4. Conclusion

The proposed BCCapDev framework allows business the flexibility and agility to very quickly identify and develop cybersecurity capabilities. The BCCapDev is a vendor neutral framework, and is not industry or business specific. By referencing the BCCapDev framework in the identification and development of cybersecurity capabilities, business will ensure that all aspects are considered where it comes to securing their environment.

5. Direction for further research

Future research will focus on the identification of capabilities which can be effectively combined to provide a single, and cheaper, yet better capability. This will be achieved through the identification of structures which has overlapping functions, such as those of a SOC or CSIRT where both provide and incident response capability. These two structures could be combined. Other business cybersecurity capabilities could also be combined with, and executed from a SOC, such as access control and data security. The identification redundant processes, and the re-use and alignment of existing processes using an enterprise architecture approach will further drive down cost.

6. References

ACM, 2016. ACM Digital Library. Available at: http://dl.acm.org/ [Accessed February 17, 2016].

Adler, M., 2007. CoBIT 4.1. Available at: http://www.isaca.org/Knowledge-Center/cobit/Documents/COBIT4.pdf.

BusinessDictionary.com, 2016. Capability. Available at: http://www.businessdictionary.com/definition/capability.html [Accessed February 16, 2016].

C. Dickerson and D. N. Mavris, 2010. *Architecture and Principles of Systems Engineering*, CRC Press.

C. Fripp, 2014. Cybercrime costs South Africa about R5.8 billion a year. Available at: http://www.htxt.co.za/2014/11/11/cybercrime-costs-south-africa-about-r5-8-billion-a-year/.

C. McNamara, 2016. Basic Overview of Various Strategic Planning Models. Available at: http://managementhelp.org/strategicplanning/models.htm [Accessed March 16, 2016].

CiteSeerX, 2016. CiteSeerX. Available at: http://citeseerx.ist.psu.edu/index;jsessionid=165FF246A77A20C39F0FDA9FA0329277 [Accessed February 17, 2016].

D. Gabel; B. Liard & D. Orzechowski, 2015. Cyber risk: Why cyber security is important. Available at: http://www.whitecase.com/publications/insight/cyber-risk-why-cyber-security-important [Accessed March 14, 2016].

ENISA, 2016. Risk Management. Available at: https://www.enisa.europa.eu/activities/risk-management [Accessed March 16, 2016].

ENISA, 2015. What is a CSIRT? Available at: https://www.enisa.europa.eu/activities/cert/support/guide2/introduction/what-is-csirt [Accessed May 18, 2015].

Furlani, C., 2011. Managing Information Security Risk: Organization, Mission, and Information System View. Available at: http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf.

Google, 2016. Google Scholar. Available at: https://scholar.google.co.za/ [Accessed February 17, 2016].

IEEE, 2016. IEEE Xplore Digital Library. Available at: http://ieeexplore.ieee.org/Xplore/home.jsp [Accessed February 17, 2016].

INCOSE, 2010. *Systems Engineering Handbook: A Guide for System Life Cycle processes and activities v3.2* C. Haskins, ed., Available at: www.incose.org/ProductsPubs/Doc/IS2010_SEHandbookv3_2_Paper.pdf.

ISACA, 2016. Risk IT Framework for Management of IT Related Business Risks. Available at: http://www.isaca.org/knowledge-center/risk-it-it-risk-management/pages/default.aspx [Accessed March 16, 2016].

ISO/IEC, 2008. Introduction To ISO 27011 (ISO27011). Available at: http://www.27000.org/iso-27011.htm.

ISO/IEC, 2009. ISO 31000 - Risk management. Available at: http://www.iso.org/iso/home/standards/iso31000.htm.

ISO/IEC, 2005. ISO/IEC 27001:2005 Information technology -- Security techniques -- Information security management systems -- Requirements. Available at: http://www.iso.org/iso/catalogue_detail?csnumber=42103.

ISO/IEC, 2011. ISO/IEC 27005:2008 Information security risk management_. Available at: http://www.iso.org/iso/catalogue_detail?csnumber=42107.

ISPA, 2016. ISPA. Available at: http://ispa.org.za/ [Accessed February 23, 2016].

ITU-T, 2008. ITU T X.1055 Risk management and risk profile guidelines for telecommunication organizations. Available at: ITU T X.1055 Risk management and risk profile guidelines for telecommunication organizations.

ITU-T, 2004. Security architecture for systems providing end-to-end communications. Available at: www.itu.int/rec/T-REC-X.805-200310-I/en.

J. Wurzler, 2013. Information Risks & Risk Management. Available at: https://www.sans.org/reading-room/whitepapers/bestprac/information-risks-risk-management-34210 [Accessed March 16, 2016].

Jacobs P., 2015. *Towards a framework for building security operation centers*. Rhodes Universtity. Available at: http://contentpro.seals.ac.za/iii/cpro/DigitalItemViewPage.external?lang=eng&sp=1017932&sp=T&suite=def.

K.B. Jensen, 1992. The Role of the Board of Directors in Setting Strategy in the Smaller Firm. Available at: http://www.ryerson.ca/~kjensen/entrepreneurship/role_board_directors.pdf [Accessed March 16, 2016].

LEADing Practice, 2016. Welcome to LEADing Practice. Available at: http://www.leadingpractice.com/ [Accessed March 17, 2016].

Live, T., 2013. 70% of South Africans have fallen victim to cyber crime. Available at: http://www.timeslive.co.za/scitech/2013/11/04/70-of-south-africans-have-fallen-victim-to-cyber-crime.

Microsoft, 2016. Microsoft Academic Research. Available at: http://academic.research.microsoft.com/?SearchDomain=2&entitytype=2 [Accessed February 17, 2016].

Minister of Justice and Correctional Services, 2015. South African Cybercrimes and Cybersecurity Bill - Draft for Public Comment. , pp.96 – 103. Available at: http://www.justice.gov.za/legislation/invitations/CyberCrimesBill2015.pdf [Accessed November 26, 2015].

NATO Cooperative Cyber Defence Centre of Excellence, 2012. *National Cyber Security Framework Manual*, Available at: https://ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf [Accessed January 29, 2016].

NIST, 2014a. Cybersecurity Framework Core. Available at: http://www.nist.gov/cyberframework/upload/framework-for-improving-critical-infrastructure-cybersecurity-core.xlsx [Accessed March 16, 2016].

NIST, 2014b. Framework for Improving Critical Infrastructure Cybersecurity. Available at: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf [Accessed March 1, 2016].

NIST, 2013. National Cybersecurity Workforce Framework. Available at: http://csrc.nist.gov/nice/framework/ [Accessed February 17, 2016].

PCI Security Standards Council, 2010. Payment Card Industry (PCI) Data Security Standards Overview. , (October). Available at: https://www.pcisecuritystandards.org/security_standards/.

R.S. Ross, 2014. Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans. *NIST Special Publication*, (August 2009), pp.1–487. Available at: papers3://publication/doi/10.6028/NIST.SP.800-53Ar4 [Accessed March 16, 2016].

S. Mukwevho, 2015. The rise of industrial espionage in SA. *ITWeb*. Available at: http://www.itweb.co.za/index.php?option=com_content&view=article&id=140594.

SANS Institute, 2013. Critical Controls for Effective Cyber Defense V 4.1. Available at: http://www.sans.org/critical-security-controls/cag4-1.pdf.

South African Government, 2013. Act No. 4 of 2013: Protection of Personal Information Act, 2013. *Government Gazette*. Available at: http://www.justice.gov.za/legislation/acts/2013-004.pdf [Accessed March 16, 2016].

South African Government, 2008. Companies Act, No 71 of 2008. Available at: http://www.acts.co.za/companies-act-2008/index.html?director.php [Accessed March 16, 2016].

Strategy&, 2012. What is a capability? Available at: http://www.strategyand.pwc.com/global/home/what-we-think/multimedia/video/mm-video_display/what-is-a-capability [Accessed February 18, 2016].

The Open Group, 2013. Welcome to TOGAF® Version 9.1 "Enterprise Edition." Available at: http://www.opengroup.org/togaf/.

TMForum, 2013. Business Process Framework. Available at: http://www.tmforum.org/BusinessProcessFramework/1647/home.html.

TOGAF, 2006. TOGAF as an Enterprise Architecture Framework. Available at: http://pubs.opengroup.org/architecture/togaf8-doc/arch/chap02.html [Accessed March 17, 2016].

W. Ulrich & W. McWhorter, 2010. Defining the Business Capability - A Cheat Sheet. *Business Architecture: The Art and Practice of Business Transformation*. Available at: http://www.bainstitute.org/resources/articles/defining-business-capability-cheat-sheet [Accessed February 16, 2016].

Weinberg, A., Agarwai, N. & Bommadervara, N., 2013. Using a plan-build-run organizational model to drive IT infrastructure objectives. *McKinsey & Company Website*, pp.2, 3. Available at: https://www.google.com/webhp?sourceid=chrome-instant&ion=1&espv=2&ie=UTF-8#q=Plan Build Run [Accessed January 5, 2016].

World Economic Forum, 2015. Global Risks 2015 10th Edition. Available at: http://www3.weforum.org/docs/WEF_Global_Risks_2015_Report15.pdf [Accessed March 14, 2016].