# A National Cybersecurity Management Framework for Developing Countries

by

**PIERRE CONRAD JACOBS**

M.Sc (Computer Science)

201516656

Submitted in fulfillment of the requirements

for the degree

**PHILOSOPHIAE DOCTOR**

in

**COMPUTER SCIENCE**

in the Faculty of Science

at the

**UNIVERSITY OF JOHANNESBURG**



Promoter: Prof. S.H. von Solms

Co-promoter: Dr. M.M. Grobler

Johannesburg

December 2018

# Executive summary

Information and Communications Technology (ICT) plays an integral role in terms of facilitating economic growth in both developed and developing countries. It is important that economic participants have confidence in the security and reliability of their partners' ICT infrastructure. As such, at a national level, a secure and reliable ICT infrastructure is seen as a national asset [1]. To facilitate the securing of the ICT infrastructure, as well as information security related services offered to citizens, nations need a National Cybersecurity Strategy (NCS). The NCS should prescribe national cybersecurity functions[1] needed to secure the nation's cyberspace.

Our experience with national cybersecurity projects showed that the management of cybersecurity at national level includes the tasks of *identifying, selecting and prioritising* cybersecurity functions, as well as the *implementation* of those functions. We conducted detailed research, and could not find existing frameworks that could be used to assist nation-states during the identification, selection, prioritisation, and implementation of national cybersecurity functions. Therefore the purpose of this thesis is to develop a National Cybersecurity Management Framework that could be used by nation states to manage its national cybersecurity functions. This framework will be broad enough to be applied by both developed and developing countries. The illustrative application of the framework in this thesis is presented in the context of developing countries, building on our experience in applying national cybersecurity solutions in South Africa as a developing country.

Effective cybersecurity function management at national level requires that the identified, selected and prioritised cybersecurity functions are implemented and offered from existing cybersecurity structures, or where no structures exist, a newly developed national cybersecurity structure. We will illustrate the application of the implementation part of our framework through the establishment, and implementation of a new national cybersecurity structure. This structure will be described with three models. The first model describes how to build the structure, the second model describes the operation of the structure, and the third model describes the monitoring of the structure's maturity.

Figure 3 on page 31 shows that development of our framework and the three models describing the structure was done in alignment with the plan-build-run-monitor (PBRM) organisational approach. The framework was developed using existing standards and frameworks, as well as using input based on our experience, and lessons learnt during cybersecurity work done at national level. Using existing and scalable standards and framework, coupled with our experience at

[1] The terms "national cybersecurity functions", and "cybersecurity functions" and "functions" are used interchangeably, and will be discussed in more detail in this document.

implementing national cybersecurity solutions will ensure that our framework can scale to national level, and that it can be implemented successfully.

# Acknowledgements

Professor Basie von Solms, my gratitude and appreciation for your patience and guidance during this research project. Your knowledge, insights and inputs were of greatest value.

To Dr. Marthie Grobler, thank you for your guidance and mentorship. Without you, this work would not have been possible.

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

To my parents, Chris and Marel, thank you for the upbringing you gave me and for all the sacrifices you have made to get me where I am at today. Mom, this work is dedicated to you. I admire your courage, and for always being a pillar of strength even in the most adverse circumstances. I will never forget you.

To Oom Peet Pienaar, thank you for explaining the more complex enterprise architecture (EA) concepts to me, and also for the recommendations and input into the models developed using EA.

To Oupa Jaap and Ouma Toet, thank you for your continuous support, endless coffee and long talks.

## Note on the author

Pierre Jacobs has more than 19 years' experience in the ICT industry, of which 16 years are in information and cybersecurity. He has occupied mid-level managerial positions at South African ICT service providers and consultancy firms. During his tenure at Faritec, Pierre assisted with the building of the South African Government Computer Security Incident Response Team (CSIRT), the Electronic Communications Security (ECS) CSIRT (ECS-CSIRT) operated by the South African State Secret Service. After the completion of the contract, he managed and improved the commercial Security Operation Centre (SOC) service offering of Faritec

He assisted with the establishment of the Cybersecurity Professional Services offering at Datacentrix, and later built their commercial SOC. Pierre grew the SOC from inception to the SOC in Africa monitoring the most devices. This SOC looked after clients, such as mobile operators and state-owned companies, as well as various South African financial institutions and mines. During the same period, he was also part of the strategic team that developed the Datacentrix cloud offering where he was responsible for the design, architecture and implementation of its public cloud offering.

From consulting, he moved to the Council for Scientific and Industrial Research (CSIR) where he was part of the team responsible for the cybersecurity for a newly developed next generation network for the South African National Defence Force (SANDF). Here he also assisted with the planning, building and operationalisation of the South African national CSIRT – the Cybersecurity Hub under the auspices of the Department of Telecommunications and Postal Services. He was part of a strategic team making recommendations on the implementation of the South African National Cybersecurity Policy Framework (NCPF), and was also part of the advisory team for the establishment of the SANDF Cyber Command, and the South African Police Services (SAPS) Cybercrimes Centre. During his tenure, he worked on the SAPS Identity and Access Management (IDAM) planning.

Pierre has experience of organisational consultancy at national level. He was approached by, and worked for the Ar-Riyadh Development Authority (ADA) in the Kingdom of Saudi Arabia as part of a multi-national team where he was responsible for the cybersecurity of the Intelligence Transport System (ITS) under development. Pierre has published numerous articles on SOCs and CSIRTs, and as part of his previous studies, developed a model and framework to measure the effectiveness of SOCs. He currently works for Cisco where he assisted with building a SOC at one of South Africa's leading financial institutions.

He has several years of strategic and operational experience in the planning, building, and running of SOCs and CSIRTs, and of applying monitoring and incident handling solutions at national level.

As such, the development of a National Cybersecurity Management Framework has been a deeply personal and intimate journey.

## Note on writing style

During the writing of this thesis, a conscious decision was made to use the pronouns "we" "us" and "our". These pronouns could refer to the author, or a group of people. The intended meaning of the use of the pronouns "we", "us" and "our" should be interpreted in the context in which it is used. The reason for using the "royal we" or "us" is to allow for a better flow of the text, with the overall intention of enhancing the reading experience.

## Note on the Use of Tables and Figures

The use of tables in this thesis is common. The tables are used to logically group and display larger volumes of data. In some instances, it happens that tables break across pages. We have made a conscious decision to leave the tables as is, where they extend over more than one page. The rationale for this decision is that the intention of meaning we want to convey might be lost when we change, shorten or omit information to force a fit across a single page. Doing so might be confusing to the reader, and does not do justice to the knowledge we wish to transfer to the reader. Unless specifically indicated, all figures and tables were created by the author/

## Note on Structure of this thesis

This thesis consists of two parts. The first part, “Part 1” describes the National Cybersecurity Management Framework (NCMF). The second part, Part 2 provides a best practice implementation guide for national cybersecurity structures. The development of the NCMF in Part 1 is our primary effort, and the reader should focus most of his/her time and reading effort on this part. Part 2 describes our best practice guide for the implementation of national cybersecurity structures through Appendices E to G. Part 2 is more technical and operational in nature, and the reader may choose not to spend as much time reading Part 2.

## Table of Contents

# PART 1

# A National Cybersecurity Management Framework

## List of Figures

# List of Tables

# Acronyms

| | |
|---|---|
| **ACM** | American computing machinery |
| **BCCAPDEV** | Business cybersecurity capability development framework |
| **BCM** | Business continuity management |
| **BCP** | Business continuity plan |
| **BIAN** | Banking industry architecture network |
| **BSI** | British Standards Institute |
| **CERT** | Computer emergency response team |
| **CI** | Counter intelligence |
| **CIC** | Cyber Intelligence centre |
| **CII** | Critical information infrastructure |
| **CIIP** | Critical Information Infrastructure Protection |
| **CISO** | Chief Information Security Officer |
| **C2M2** | Cybersecurity Capability Maturity Model |
| **CMM** | Capability Maturity Model |
| **CMU** | Carnegie Mellon University |
| **COBIT 5** | Control Objectives for Information Technology version 5 |
| **COTS** | Commercial Off The Shelf |
| **CRC** | Cyber Response Committee |
| **CSIR** | Council for Scientific and Industrial Research |
| **CSIRT** | Computer Security Incident Response Team |
| **CSOC** | Cybersecurity Operations Center |
| **DAP** | Defence Acquisition Policy |
| **DIRCO** | Department of International Relations and Cooperation |
| **DNS** | Domain Name Server |
| **DOD** | Department of Defence |
| **DOJ** | Department of Justice |

| | |
|---|---|
| **DOTMLF** | Doctrine, Organizations, Training, Materiel, Leadership, Personnel and Facilities |
| **DPSA** | Department of Public Service and Administration |
| **DST** | Department of Science and Technology |
| **DTPS** | Department of Telecommunications and Postal Services |
| **EA** | Enterprise Architecture |
| **E-CMIRC** | Early Cybersecurity Monitoring and Incident Response Center |
| **E-CMIRC CDM** | Early Cybersecurity Monitoring and Incident Response Center Capability Development Model |
| **E-CMIRC CMM** | Early Cybersecurity Monitoring and Incident Response Center Capability Maturity Model |
| **E-CMIRC OM** | Early Cybersecurity Monitoring and Incident Response Center Operations Model |
| **ECS-CSIRT** | Electronic Communications Security Computer Security Incident Response Team |
| **ECT** | Electronic Communications and Transactions |
| **EISA** | Enterprise Information Security Architecture |
| **ENISA** | European Union Agency for Network and Information Security |
| **IEEE** | Institute of Electrical and Electronics Engineers |
| **IETF** | Internet Engineering Task Force |
| **eTOM** | Enhanced Telecom Operations Map |
| **FBI** | Federal Bureau of Investigation |
| **FIM** | File Integrity Monitoring |
| **FIRST** | Forum of Incident Response and Security Teams |
| **HoD** | Head of Department |
| **IBM** | International Business Machines |
| **IAA** | Insurance Application Architecture |
| **ICASA** | Independent Communications Authority of South Africa |
| **ICT** | Information and Communications Technology |
| **IDS** | Intrusion Detection System |
| **ISACA** | Information Systems Audit and Control Association |

| | |
|---|---|
| **ISG** | Information Security Group |
| **ISO/IEC** | International Organization for Standardization (ISO) International Electrotechnical Commission (IEC) |
| **IPS** | Intrusion Prevention System |
| **ISP** | Internet Service Provider |
| **ITGI** | IT Governance Institute |
| **ITIL** | Information Technology Information Library |
| **ITU** | International Telecommunications Union |
| **JCPS** | Justice, Crime Prevention and Security |
| **KISA** | Korean Internet and Security Agency |
| **MOE** | Measure of Effectiveness |
| **MOP** | Measure of Performance |
| **MPSS** | Minimum Physical Security Standards |
| **NATO** | North Atlantic Treaty Organisation |
| **NCAC** | National Cybersecurity Advisory Council |
| **NCMF** | National Cybersecurity Management Framework |
| **NCPF** | National Cybersecurity Policy Framework |
| **NCS** | National Cybersecurity Strategy |
| **NDMC** | National Disaster Management Center |
| **NERSA** | National Energy Regulator of South Africa |
| **NGOSS** | New Generation Operation Systems and Software |
| **NICE** | National Initiative for Cybersecurity Education |
| **NIST** | National Institute of Standards and Technology |
| **NSA** | National Security Agency |
| **NTP** | Network Time Protocol |
| **OAS** | Organization of American States |
| **OCSIA** | Office of Cyber Security and Information Assurance |
| **OECD** | Office of Economic Cooperation and Development |
| **O&M** | Operations and Maintenance |
| **openSAMM** | Software Assurance Maturity Model |

| | |
|---|---|
| **OS** | Operating System |
| **PBRM** | Plan-Build-Run-Monitor |
| **PCI-DSS** | Payment Card Industry Data Security Standard |
| **PFMA** | Public Finance Management Act |
| **PKI** | Public Key Infrastructure |
| **PLC** | Programmable Logical Controllers |
| **POSTEDFIT-B** | Personnel, Organisation, Sustainment, Training, Equipment, Doctrine, Facilities, Information, Technology and Budget |
| **R&D** | Research & Development |
| **SABRIC** | South African Banking Risk Center |
| **SACSA** | South African Communications Security Agency |
| **SANDF** | South African National Defence Force |
| **SANS** | SysAdmin, Audit, Networking, and Security |
| **SAPS** | South African Police Services |
| **SACSA** | South African Communications Security Agency |
| **SCADA** | Supervisory Control and Data Acquisition |
| **SE** | Systems Engineering |
| **SEBoK** | Systems Engineering Body of Knowledge |
| **SEI** | Software Engineering Institute |
| **SFIA** | Skills Framework for the Information Age |
| **SID** | Shared Information and Data |
| **SIEM** | Security Incident and Event Monitoring |
| **SITA** | State Information Technology Agency |
| **SME** | Small and Medium-sized Enterprises |
| **SOC** | Security Operations Center |
| **SOE** | State Owned Entity |
| **SSA** | State Security Agency |
| **SSE-CMM** | Systems Security Engineering Capability Maturity Model |
| **TAM** | Telecom Application Map |

| | |
|---|---|
| **TEPID-OIL** | Training, Equipment, Personnel, Infrastructure, Doctrine and concepts, Organization, Information, Logistics |
| **TMForum** | Telemanagement Forum |
| **TNA** | Technology Neutral Architecture |
| **TOM** | Telecom Operations Map |
| **USA** | United States of America |
| **UK** | United Kingdom |
| **VM** | Virtual Machine |
| **WoG** | Whole of Government |
| **WoN** | Whole of Nation |
| **WoS** | Whole of Systems |

# PART 1

# The National Cybersecurity Management Framework (NCMF)

# Chapter 1: Introduction

## 1.1 Introduction

To facilitate the identification, selection, prioritisation and implementation of national cybersecurity functions, the **N**ational **C**ybersecurity **M**anagement **F**ramework (**NCMF**) is developed. The significance of the NCMF is that it would improve a nation state's cybersecurity posture and that it offers value in terms of cost and skills saving. This thesis presents one framework, with the purpose to assist nation states with the national cybersecurity management tasks of identifying, selecting, prioritising, and implementing national cybersecurity functions. In developing the framework, the **p**lan-**b**uild-**r**un-**m**onitor (**PBRM**) organisational approach is followed as an overall guiding framework. The aim of the framework and structure is to improve the national cybersecurity posture of developing countries. This framework is developed keeping in mind the unique requirements and constraints of developing countries. Developing countries have unique requirements in terms of the burden placed on available financial and skills resources where it concerns their national cybersecurity efforts.

The NCMF satisfies the "Plan" function of the PBRM organisational approach, and we will apply the NCMF in Chapter 4 to identify, select and prioritise general[1] cybersecurity functions. An illustrative application of the implementation part of the NCMF will be provided through a proposed best practice guide for the implementation of national cybersecurity structures in Part 2 of this thesis. Our best practice guide describes the establishment of a new national cybersecurity structure by selecting two of the identified cybersecurity functions to be used for the development of an initial cybersecurity structure. The two selected functions are the *incident handling*, and the *monitoring and evaluation* function. The functions are realised by services offered from national cybersecurity structures. The *incident handling* function is offered from a computer security incident response team (CSIRT) structure, while the *monitoring and evaluation* function is offered from a security operation centre (SOC) structure. CSIRTs and SOCs offer multiple cybersecurity services to realise the *incident handling* and *monitoring and evaluation* functions.

Our best practice guide describes the establishment of a new structure called the **E**arly **C**ybersecurity **M**onitoring and **I**ncident **R**esponse **C**enter (**E-CMIRC**), from where the services of the two functions are combined to realise a cost and skills saving for developing countries. The newly conceived E-CMIRC structure is described with three models. To satisfy the *"build"* function of the PBRM organisational approach, the E-CMIRC Capability Development Model (E-CMIRC CDM) is developed. The E-CMIRC CDM is a symbolic model describing the building of the E-CMIRC structure. The E-CMIRC Operations Model (E-CMIRC OM) is a symbolic model describing E-CMIRC operations and satisfies the *"run"* function of the PBRM organisational approach. The E-CMIRC CDM and the E-CMIRC OM is presented as a single integrated model. The *"monitor"*

[1] General cybersecurity functions are by definition non-mandatory

function of the PBRM organisational approach is satisfied through the development of the E-CMIRC Capability Maturity Model (E-CMIRC CMM) which is a symbolic model describing how the maturity of the E-CMIRC can be measured, and improved on.

## 1.2 Background

Where it concerns the establishment of a secure ICT infrastructure, the needs of developing countries are different from those of developed countries. During the establishment of an ICT infrastructure, security and reliability must be considered throughout the whole process.

Most developed countries, such as the Office of Economic Cooperation and Development (OECD) nation-states, have developed and implemented National Cybersecurity Strategies (NCSs). Examples of developed countries with existing National Cybersecurity Strategies are the United States of America (USA), with their *"National Strategy to Secure Cyberspace"* [2] and the United Kingdom (UK) with their *"National Cybersecurity Strategy 2016 to 2021"* [3].

Some developed nation-states, such as the USA, augments its National Cybersecurity Strategy (NCS) with Presidential Directives and national cybersecurity policies. These National Cybersecurity Strategies, policies and directives govern cybersecurity activities at national level. They also list national cybersecurity functions applicable to their specific countries. A list of the OECD nation states (all developed countries) with their NCSs may be found by following this link https://goo.gl/stoUct, and a list of European Union (EU) countries (also developed countries) with their NCSs may be found here https://goo.gl/1EN6GE.

Developing countries have unique challenges in that they often do not have sufficient funds, or resources available to secure their ICT infrastructure. It is further our experience that developing countries often have not yet developed NCSs. There are however exceptions, such as Kenya with their *"Cybersecurity Strategy"* [4], Nigeria with their *"National Cybersecurity Strategy"* [5] and South Africa with their *"National Cybersecurity Policy Framework"* (NCPF) [6].

The NCSs and policies of developed and developing countries all describe different elements making up a nation's cybersecurity efforts. One of the elements described in the NCSs, is national cybersecurity functions. National cybersecurity functions are provided by cybersecurity services that deliver on a function. Cybersecurity services,[2] in turn, consists of national cybersecurity capabilities.[3] The relationship between national cybersecurity functions, services, capabilities and structures is shown in Figure 1.

[2] In this thesis, the terms "cybersecurity services" and "services" are used interchangeably.

[3] In this thesis, the terms "cybersecurity capabilities" and "capabilities" are used interchangeably.

Figure 1 shows that national cybersecurity functions are realised through national cybersecurity services. National cybersecurity services, in turn, are made up of national cybersecurity capabilities that consist of people, processes and technology. The national cybersecurity functions and their enabling cybersecurity services are offered from national cybersecurity structures. Where no national cybersecurity structures exist, new national cybersecurity structures must be conceived and developed.

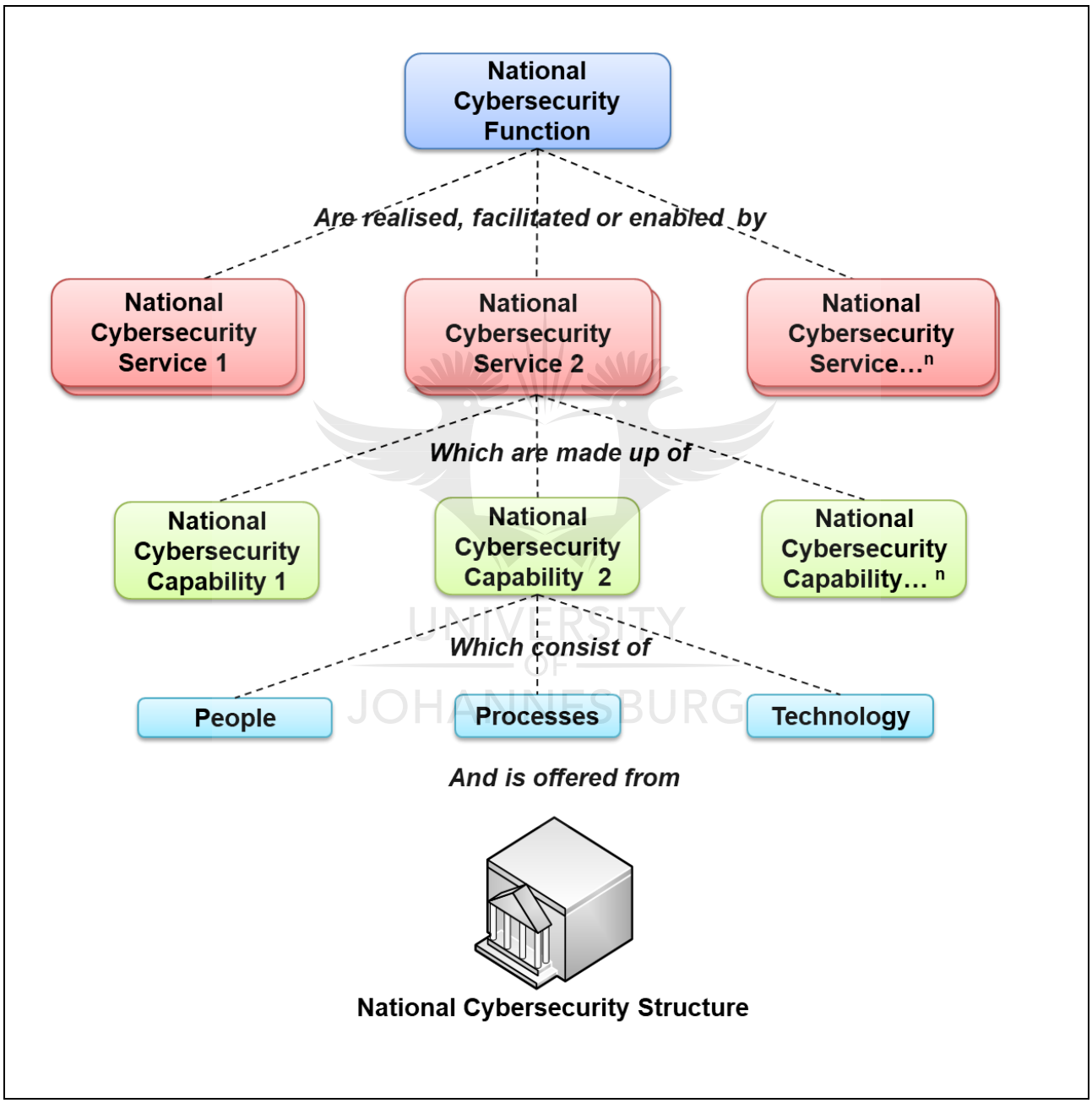



**Figure 1: Relationship between cybersecurity functions, services, capabilities and structures** [7]

## 1.3 Motivation

Based on our experience, we have identified four tasks that need to be executed during the management of national cybersecurity functions. Going forward in this thesis, the term "*management*" – in the context of the development of the national cybersecurity management framework – must be understood to serve as an umbrella term that includes the four tasks. The four national cybersecurity management tasks will now be introduced in the text below.

- **Task 1:** To **identify** national cybersecurity functions.

To achieve the *"identification of national cybersecurity functions"* task, a nation-state should have a framework to follow, to identify mandatory or non-mandatory national cybersecurity functions. Such a framework should be broad enough to identify cybersecurity functions for both developed and developing countries. The framework should further be broad enough to identify cybersecurity functions at a national and organisational level. Our experience showed that most often nation states will focus their national cybersecurity efforts on critical infrastructures, and these are most often state owned entities (SOEs). The identification task identifies all elements that influence and inform the identification of national cybersecurity functions. Some of these elements are national and international normative and authoritative sources, dimensions, domains and mandates. This task then uses the elements to identify a nation's mandatory, or non-mandatory cybersecurity functions.

- **Task 2:** To **select** national cybersecurity functions for implementation.

This task uses the elements identified in Task 1 to guide the "*selection of national cybersecurity functions"*. Task 1 results in a list of cybersecurity functions identified for possible implementation at the national level. From this list, it is recommended that nation-states select functions for implementation. Nations with limited capacity and capability may use existing national and international normative and authoritative sources, dimensions, domains and mandates to guide the selection of their national cybersecurity functions for implementation. Most nation states and specifically developing countries will not have the necessary resources to implement a multitude of the identified functions. Therefore, we recommend that one, or at most two, national cybersecurity functions are selected for implementation. During Task 2, functions are selected for implementation at the national level.

- **Task 3:** To **prioritise** national cybersecurity functions.

Once a list of selected cybersecurity functions has been compiled, their implementation needs to be prioritised. Task 3 assists with the "*prioritisation of national cybersecurity functions"* for implementation. This task may be executed by following a National Strategic Risk and Threat Assessment approach, such as the strategy described in the National Institute of Standards and Technology (NIST) Cybersecurity Framework, or

standards such as ISO/IEC 27005:2011 [8], [9] or ISO/IEC 3100:2009 [10]. While the outcome of the National Strategic Risk and Threat Assessment influences the selection of national cybersecurity functions, its primary purpose is to prioritise the national cybersecurity functions for implementation.

There is a reciprocal relationship between the selection and prioritisation tasks. The National Strategic Risk and Threat Assessment approach influences the selection, and prioritises the national cybersecurity functions for implementation, while the dimensions, mandates and domains may also influence the selection and prioritisation of national cybersecurity functions for implementation.

- **Task 4:** To **implement** national cybersecurity functions.

The fourth task, "*national cybersecurity function implementation*", is the *implementation of national cybersecurity functions*. The implementation task should be broad enough to guide the implementation of any nation state's mandatory or general cybersecurity function. The tasks are displayed in Figure 2. Figure 2 shows that the dimensions, mandates and domains may influence and inform the identification of national cybersecurity functions. As an example, the national cybersecurity function requirements will differ when a nation is at war (the Offensive domain) or in time of peace (Defensive domain). The dimensions, domains and mandates may also influence the selection and prioritisation tasks. The arrows looping between the selection and prioritisation tasks show that the selection task of the NCMF will be influenced mainly by the National Strategic Risk and Threat Assessment approach. It also shows that the prioritisation task is influenced by the cybersecurity dimensions, mandates and domains (introduced in Chapter 3).

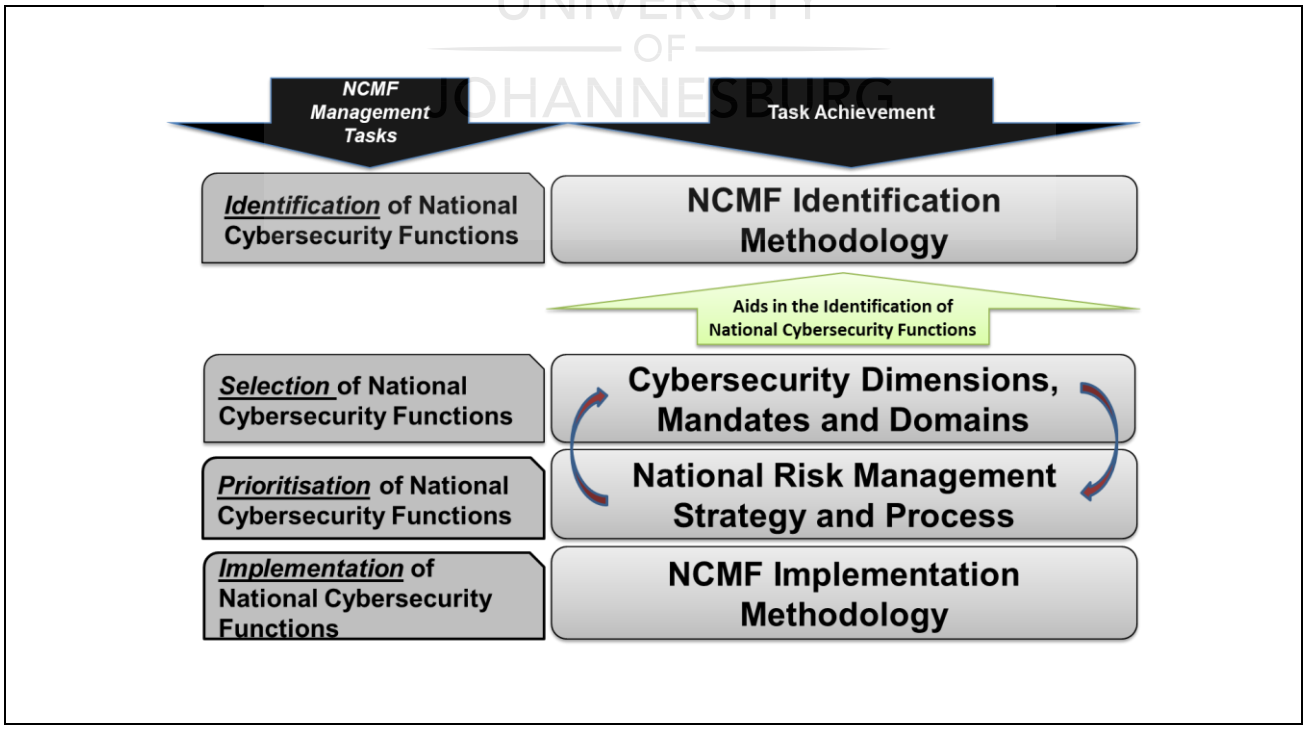



**Figure 2: National Cybersecurity Management Framework Tasks**

In an ideal situation, there would be guidance in the form of a national framework to direct, steer and drive nation-states during the management of their national cybersecurity functions. Detailed research conducted by us have shown that no national cybersecurity management framework is publicly available.

The lack of a national framework to guide nation-states during the management of national cybersecurity functions could lead to disjointed efforts between state departments and actors. Also, not using a framework when managing national cybersecurity functions could result in outcomes that are not relevant to a nation state's cybersecurity functional requirements or outcomes, and results that are inconsistent, and not repeatable or measurable. It could further lead to elements related to the management of national cybersecurity functions being overlooked. It is also difficult to demonstrate national cybersecurity intent and effort if there is no framework to measure progress against.

The Association for Computing Machinery (ACM) [11], CiteSeerx [12], Google Scholar [13], Institute of Electrical and Electronics Engineers (IEEE) [14] and Microsoft Academic Research [15] were consulted in this research, all being strong sources of literature in this area. No national cybersecurity management framework could be found. Neither could a best practice guide describing the implementation of national cybersecurity structures that offer a combination of services from multiple functions, be found.

Considering the motivation for a national cybersecurity management framework to direct, steer and drive nation-states during the management of their national cybersecurity functions, a strong case can be made that nation-states need:

1. A National Cybersecurity Management Framework (NCMF) that assists them during the identification, selection, prioritisation, and implementation of national cybersecurity functions and its structures.

2. A best practice guide that describes the implementation of national cybersecurity structures from where the selected and prioritised national cybersecurity functions, identified through the application of the National Cybersecurity Management Framework, are offered from.

A framework that can be used during the management of cybersecurity functions, at the national level, would be helpful and is advantageous in that following a framework ensures that all elements playing a role in the management of national cybersecurity functions are considered. Examples of elements influencing the identification, selection and prioritisation of national cybersecurity functions are national and international authoritative and normative sources, the dimensions (actors and stakeholders), domain of national cyber operations, and the national mandate to act in a specific way.

Such a National Cybersecurity Management Framework would further provide a systematic and structured approach during the management of national Cybersecurity functions and provide a mechanism to facilitate budgeting estimates for the implementation of national cybersecurity functions. Nation-states thus need a

***N**ational **C**ybersecurity **M**anagement **F**ramework* to guide and steer them during the identification, selection, prioritisation, and implementation of national cybersecurity functions that are applicable, and specific to their countries. The aim of such a NCMF will be to improve a nation's national cybersecurity posture. A NCMF should also be broad enough to be used by both developed and developing countries, and it should be flexible enough to be applied at both national and organisational level. Based on our experience, some of the characteristics that we would like to attribute to a NCMF are:

- A NCMF must be able to *scale* to national level, while keeping international influences into consideration.
- A NCMF must be *flexible* in order for it to adjust to changes in the nation states' national, geopolitical and cybersecurity environment and resulting requirements.
- A NCMF must be *agile* to guarantee a timeous response to cyber threats and changes in the nation state's cybersecurity posture, and cybersecurity function requirements.

With our experience in implementing frameworks at the national level, we have realised that any national framework with too many levels or steps are cumbersome and difficult to implement. Our experience, and coupled with these characteristic, impose a limit on the number of levels or steps that makes up an NCMF. Many levels or steps open up the framework for misinterpretation and make it difficult to implement the framework and measure progress.

Experience further indicated that national frameworks need to be kept as simple as possible. This must be done in order to simplify its understanding and to allow the nation-state using the framework to quickly show progress and gains where it concerns the improvement of its national cybersecurity. Our NCMF intends to consider the needs and constraints of developing countries. Where it concerns the securing of national ICT assets and infrastructure, developing countries are constrained in terms of fiscal and skills resources.



It may thus not be possible for developing countries to implement all the national cybersecurity functions that they identify with an NCMF. It is our experience that developing countries should start small, and follow a structured and phased approach when securing their national ICT assets and infrastructure. Taking into consideration their constraints, and based on our experience, it is recommended that developing countries only select one, or at most, two national cybersecurity functions for implementation at a time.

Developing countries should further attempt to identify the overlapping services and technologies of their national cybersecurity functions, and combine these. Combining the services and technologies allows for one set of skills to be used to implement more than one function, and possibly use a single technology to enable more than one function. The cybersecurity services and technologies common to the selected national cybersecurity functions could be offered from a single, initial or start-up national cybersecurity structure to realise savings in terms of cost and skills needed.

Developing countries thus also need a best practice guide describing the implementation of an ***early or start-up national cybersecurity structure*** from where common service processes and technologies are offered, which realises one, or two at the most, national cybersecurity functions. Combining common processes and technologies results in a cost saving. In doing so, developing countries will improve their national cybersecurity posture, while taking into consideration their fiscal and skills resource constraints.

As part of this study, we will develop such a best practice guide. We call this structure an "*early*" structure since, for many developing nations, this will be the first national cybersecurity structure to be established. The intention is further that more functions may be added to, and offered from the *"early"* structure as the nation state's cybersecurity journey matures. The implementation of this early or start-up national cybersecurity structure may be guided, and governed by a framework such as the NCMF. The best practice guide describing the structure may use a model or models. A common denominator across all models is that some elements of the actual concept, or system to be constructed, are abstracted, or mapped onto the model [16]. Models can thus be used to define or imitate the mechanism and operation of a cybersecurity structure.

Using a reference model during the implementation of a national cybersecurity structure may assist with budgeting for the national cybersecurity structure and its services. Another advantage of using a model is that it provides a baseline to measure the structure's maturity against, and to ensure that consistent, repeatable and predictable results are achieved. A model describing such an initial or start-up national cybersecurity structure, offering services from multiple national cybersecurity functions - in the context of developing countries - could not be identified from existing literature. The discussion above leads to our Problem Statement.



## 1.4 Problem statement

**Research problem**

A framework, dedicated to developing countries, to assist them with the national cybersecurity management tasks of the

- identification,
- selection
- prioritisation, and
- implementation

of national cybersecurity, functions could not be identified from existing literature. We have consulted existing literature sources for reference models describing developing country-specific, initial or start-up national cybersecurity structures from where their national cybersecurity functions can be offered from. Our literature study did not reveal any such models. It is important to follow a reference framework or model during the execution of national cybersecurity management tasks. Not following a framework or model may

lead to disjointed efforts, misalignment between organs of state and state departments makes budgeting difficult, and lead to inconsistent, and non-repeatable results. This ultimately leads to wasted expenditure and a poor national cybersecurity effort.

## 1.5 Objectives

The problem statement defined in Section 1.4, leads to the following objective for this study. To address the problem, we have identified a Primary objective and a secondary objective. The two objectives are defined as follows:

**Objective**

**Primary Objective:**

To develop a scalable and flexible framework (the NCMF) that can be used by developing countries to

- Identify,
- Select,
- Prioritise, and
- Implement national cybersecurity functions.

We will illustrate the implementation part of the NCMF by proposing a best practice guide to be used during the implementation of new, national cybersecurity structures. This best practice guide will describe the national structure with three models. This leads to our Secondary Objective.



**Secondary Objective:**

To develop a comprehensive best practice guide that may be used during the implementation of national cybersecurity structures. We will develop three models as part of this best practice guide to describe the implementation of national cybersecurity structures.

## 1.6 Approach

The primary aim of this study is to provide a framework that can be used by developed and developing countries to improve their national cybersecurity posture in an effective, and cost and skills-efficient way. This framework is called the National Cybersecurity Management Framework (NCMF), and provides a framework to assist with the national cybersecurity management tasks.

To illustrate the application of the implementation part of the NCMF, and as a secondary objective, a comprehensive best practice guide is developed that describes the implementation of national cybersecurity structures. The best practice guide will describe a newly conceived national cybersecurity structure with three

reference models: a capability development model (CDM), an operational model (OM) and a capability maturity model (CMM). This new structure is called the E-CMIRC (developed in Part 2 of this thesis). The **p**lan-**b**uild-**r**un-**m**onitor (**PBRM**) organisational approach is used as an overall guide to group the NCMF and E-CMIRC development activities. The approach is displayed in Figure 3.

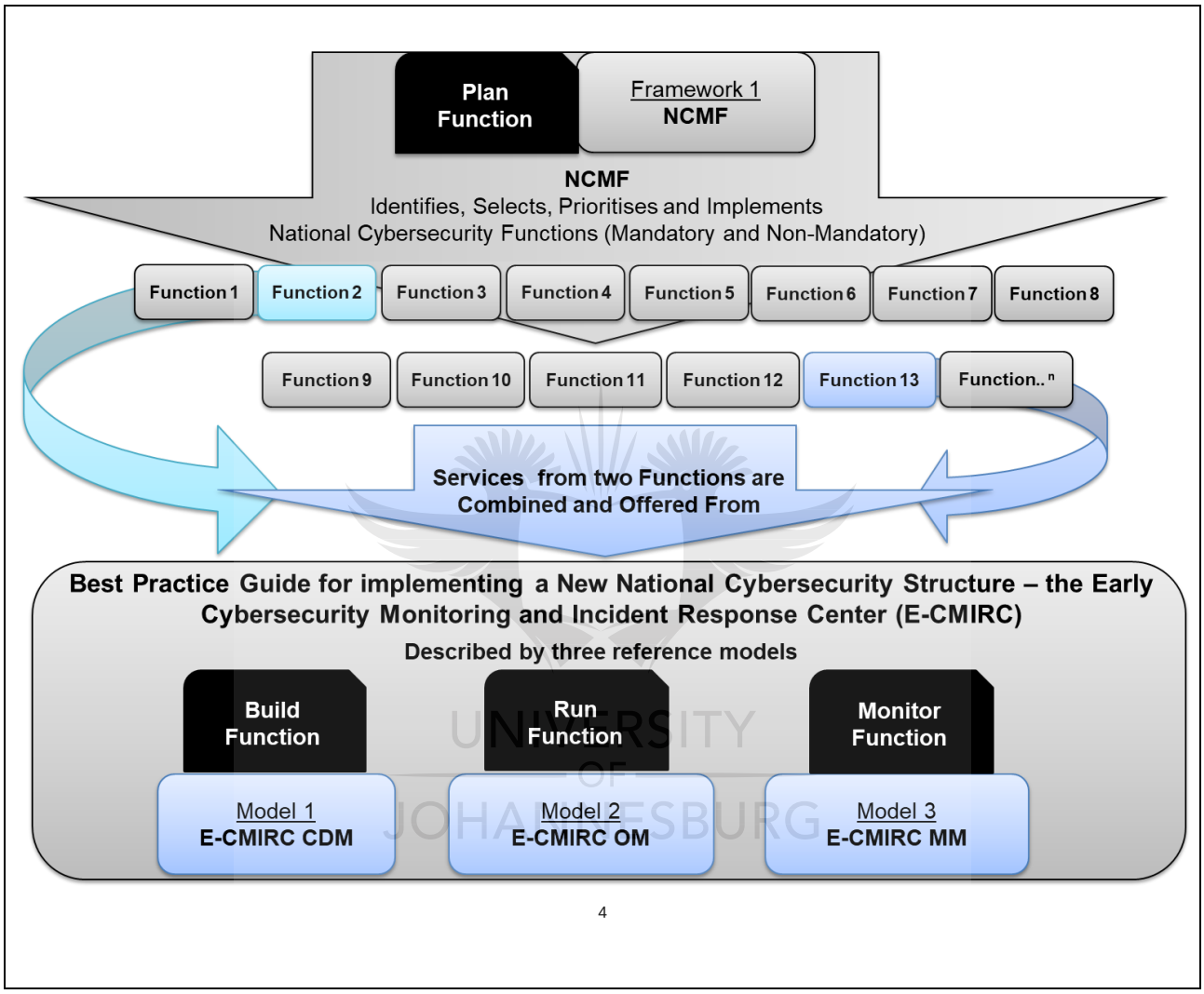



**Figure 3: Relationship Between NCMF and E-CMIRC**

Figure 3 illustrates that the NCMF will be applied to identify general or non-mandatory cybersecurity functions that are general in nature. We will use the NCMF in Chapter 3 to identify the general cybersecurity functions. We also illustrate that we will select two of the general functions, and identify their services and technologies with the intention of combining them, and then offer them from a newly envisioned national cybersecurity structure. This new structure, called the E-CMIRC, is described with three reference models. The first model

[4] The general cybersecurity functions are discussed in detail in Chapter 3.

is the E-CMIRC Capability Development Model (CDM), describing the development of the structure. The second model is the E-CMIRC Operations Model (OM), describing the E-CMIRC operations. The third model is the E-CMIRC Maturity Model, describing the monitoring of the E-CMIRC structure's maturity.

We will now, in Section 1.7 introduce the approach we will follow to develop the NCMF. Our approach consist of five high-level steps, and these are discussed in more detail in the section following.

## 1.7 NCMF development approach

The NCMF will be developed using the approach described in the following five steps.

**Step 1:** Identify an overarching, high-level organisational approach to be used to guide, but also constrain the development and scope of the NCMF. This overarching organisational approach will guide and steer the development of the NCMF and national structures. Our selected approach is discussed in Section 2.3.

**Step 2:** Identify primary elements that could serve as input into the NCMF to aid in the identification of national (mandatory and non-mandatory) cybersecurity functions. These elements are national and international authoritative and normative sources applicable to the nation-state that applies the NCMF. The primary elements are introduced in Section 2.6.

**Step 3:** Consider secondary elements that may influence the identification, selection and prioritisation of national cybersecurity functions. These are elements such as cybersecurity dimensions, mandates and domains. Dimensions describe the element or factor making up an entity, such as national cybersecurity, as well as its actors, while domains describe what actions can take place in a nation's cyber environment. Mandates give the nation-state the authority to act in a specific way on its cybersecurity effort. Cybersecurity dimensions, mandates and domains are discussed in detail in Chapter 3 and influences, and informs the selection and prioritisation tasks

**Step 4:** Consideration has to be given to the implementation, and monitoring of the NCMF as a framework itself, as well as the implementation of national cybersecurity functions. To achieve this, a national coordinating and controlling body needs to be put in place to manage the implementation and monitoring of the framework at the national level, and also to oversee the coordination of the implementation of national cybersecurity functions. The overall controlling body is introduced and is discussed in Section 5.4.

**Step 5:** The development of the NCMF satisfies the plan function of the PBRM organisational approach in that the NCMF provides a framework that can be used to plan the execution of the cybersecurity management tasks. The mapping of the NCMF to the PBRM organisational approach is shown in

Figure 6 and described in Section 1.9. Once the national cybersecurity functions are identified, national cybersecurity structures are needed to offer those functions from. Step 5 identifies these national cybersecurity structures, and where none exists, envisions new national cybersecurity structures. The national cybersecurity structures are identified and discussed in Section 5.3.3.

Our NCMF development approach is shown in Figure 4.

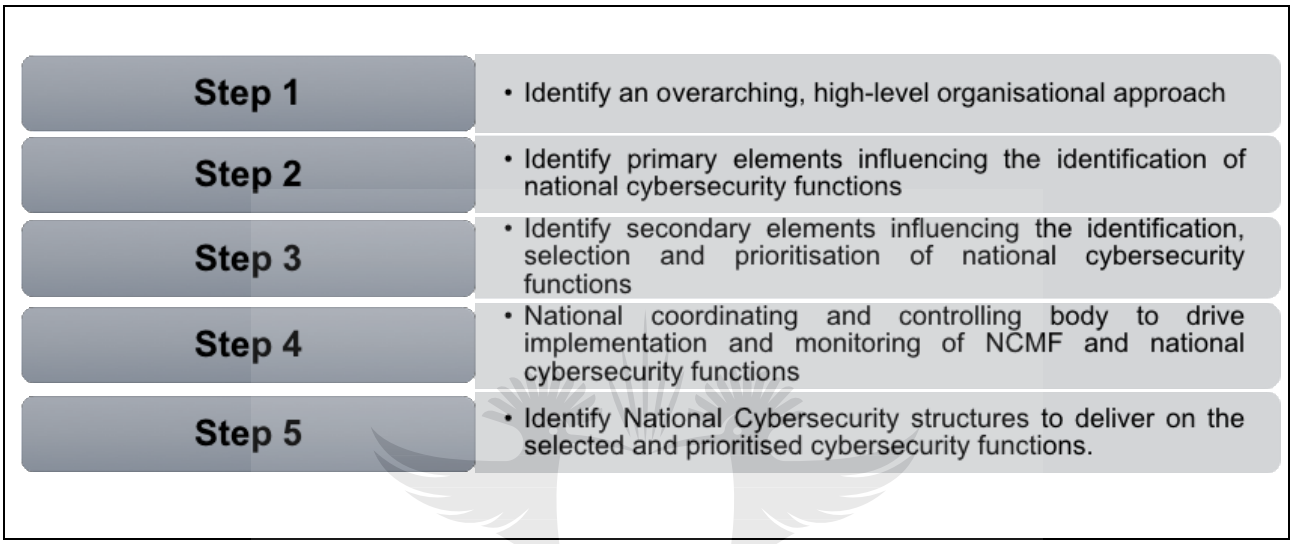



**Figure 4: NCMF development approach**

## 1.8 Best practice guide for implementing national cybersecurity structures

Our best practice guide will be used to illustrate and explain the implementation part of the NCMF by demonstrating the implementation of a new national cybersecurity structure. The E-CMIRC is such a newly envisioned, national cybersecurity structure. We will use the NCMF implementation part as guidance for the implementation of the E-CMIRC, while following the PBRM organisational approach. The NCMF satisfies the Plan function of the PBRM organisational approach while the E-CMIRC will be described with three models, satisfying the Build, Run and Monitor functions of the PBRM organisational approach. We will describe our E-CMIRC with three models. The E-CMIRC and its descriptive models are developed using the approach described in the following steps.

**Step 1:** Through the application of the NCMF, the most general cybersecurity functions will be identified. This will be achieved by identifying mandatory prescripts in national and international authoritative sources, as well as non-mandatory recommendations in national and international normative sources. From the functions identified, we will then identify the most commonly occurring functions to compile a list of general cybersecurity functions. The general functions are identified in Chapter 4.

In Section 1.3, we made the statement that it would not be viable for developing countries to implement all the identified national cybersecurity functions at once. The recommendation was made that developing countries should start small and follow a phased approach. Following these recommendations, only two of the general cybersecurity functions that will be identified during an illustrative application of the NCMF will be selected to develop the E-CMIRC by merging their services and technologies. The two selected functions are introduced in Sections 4.6.7 and 4.6.8, and are discussed in detail in Appendix B and Appendix C.

**Step 2:** Existing cybersecurity structures offering the two selected national cybersecurity functions' services are identified. The two structures' functions are identified, analysed, and a combination of their functions is selected for the E-CMIRC. The identification of the two structure's functions are done in Appendices B and C and combined for the E-CMIRC in Appendix D.

**Step 3:** The services and technologies that deliver the functions offered from the two existing structures (which we will identify in Step 2) are identified and merged in Appendix D and a new national cybersecurity structure, the E-CMIRC is developed from where the merged cybersecurity services are offered from. In following the PBRM organisational approach, three models are developed to describe the E-CMIRC. The three models satisfy the build, run and monitor functions of the PBRM organisational approach as displayed in Figure 3.

**Step 4:** In the fourth step, we will develop the first model. This model describes the development of the E-CMIRC structure and is called the E-CMIRC Capability Development Model (E-CMIRC CDM). This model satisfies the build function of the PBRM organisational approach and is developed in Appendix E.



**Step 5:** In the fifth step, we develop the second model, and it describes the operationalisation of the E-CMIRC. This model is named the E-CMIRC Operations Model (E-CMIRC OM), and satisfies the Run function of the PBRM organisational approach. This model is developed in Appendix F.

**Step 6:** The third model is developed in step 6, and it describes how to measure and monitor the E-CMIRC's capability maturity. This model is named the E-CMIRC Capability Maturity Model (E-CMIRC CMM). We develop this model in Appendix G.

Our best practice guide development approach is shown in Figure 5.

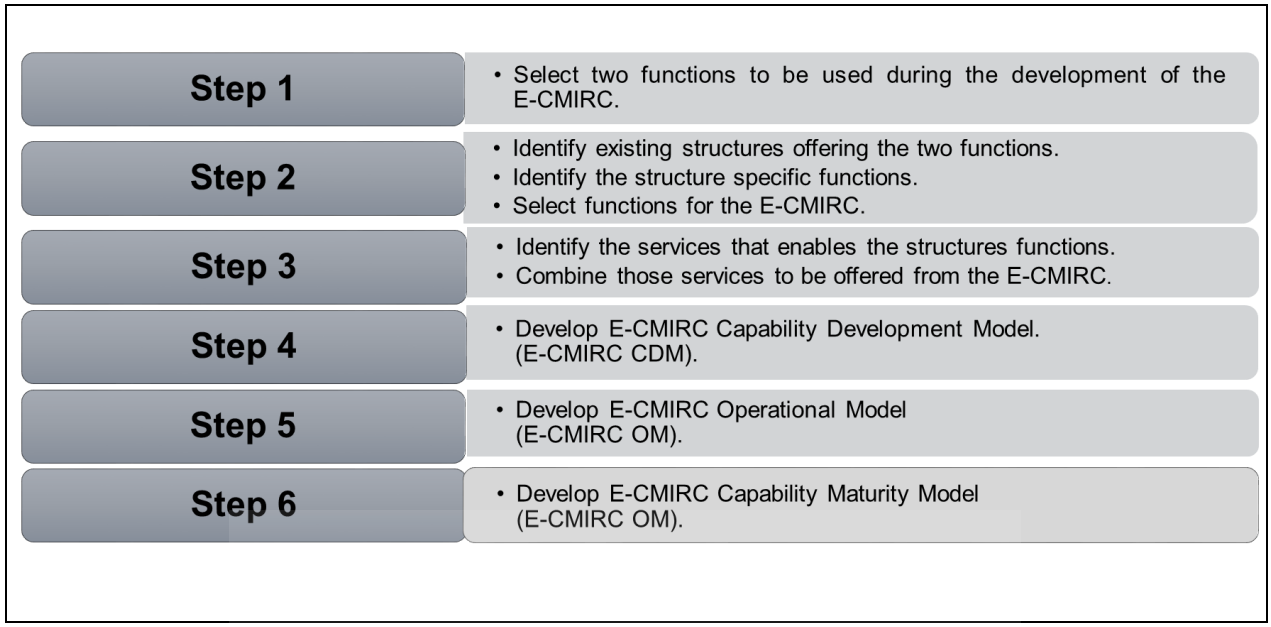



**Figure 5: E-CMIRC development approach**

Step 1 in Figure 5 shows that we will select two functions from the general and non-mandatory national cybersecurity functions we will identify in Chapter 3, to be used during the development of our E-CMIRC. In step 2 we will identify the two existing cybersecurity structures that deliver on the two selected national functions. Once we have identified the two structures, we will identify the structure-specific functions, and make a selection of the two structure's functions to be offered by our E-CMIRC. In step 3 we identify the services that enable the structures functions, and make a selection of services to be offered from our E-CMIRC. We develop the E-CMIRC descriptive models during step 4 to step 6.



## 1.9 Deliverables

The **primary deliverable** to realise the objectives in Section 1.5 will, therefore, be an NCMF that can be used during the identification, selection, prioritisation, and implementation of cybersecurity functions. The framework provides a methodology to be followed during the management of cybersecurity functions. The NCMF *identification* part will be used to identify sources describing mandatory and non-mandatory cybersecurity functions.

**Primary deliverable**

The primary deliverable is a national cybersecurity management framework, the **N**ational **C**ybersecurity **M**anagement **F**ramework (**NCMF**).

To illustrate the application of the "*national cybersecurity function implementation"* part of the framework (See Task 4), two of the identified general cybersecurity functions will be selected, and a best practice guide is proposed that describe the implementation of our new national cybersecurity structure, the E-CMIRC. Our implementation guide will describe this newly proposed national cybersecurity structure, with three models. The three models will be developed to describe the building, running and monitoring of the E-CMIRC structure.

## Secondary deliverable

The secondary deliverable is comprehensive a best practice guide that describes the implementation of national cybersecurity structures. We will describe the implementation of a new structure called the **E**arly **C**ybersecurity **M**onitoring and **I**ncident **R**esponse **C**enter (**E-CMIRC**). It is described using three reference models.

The primary and secondary deliverables are displayed in Figure 6.

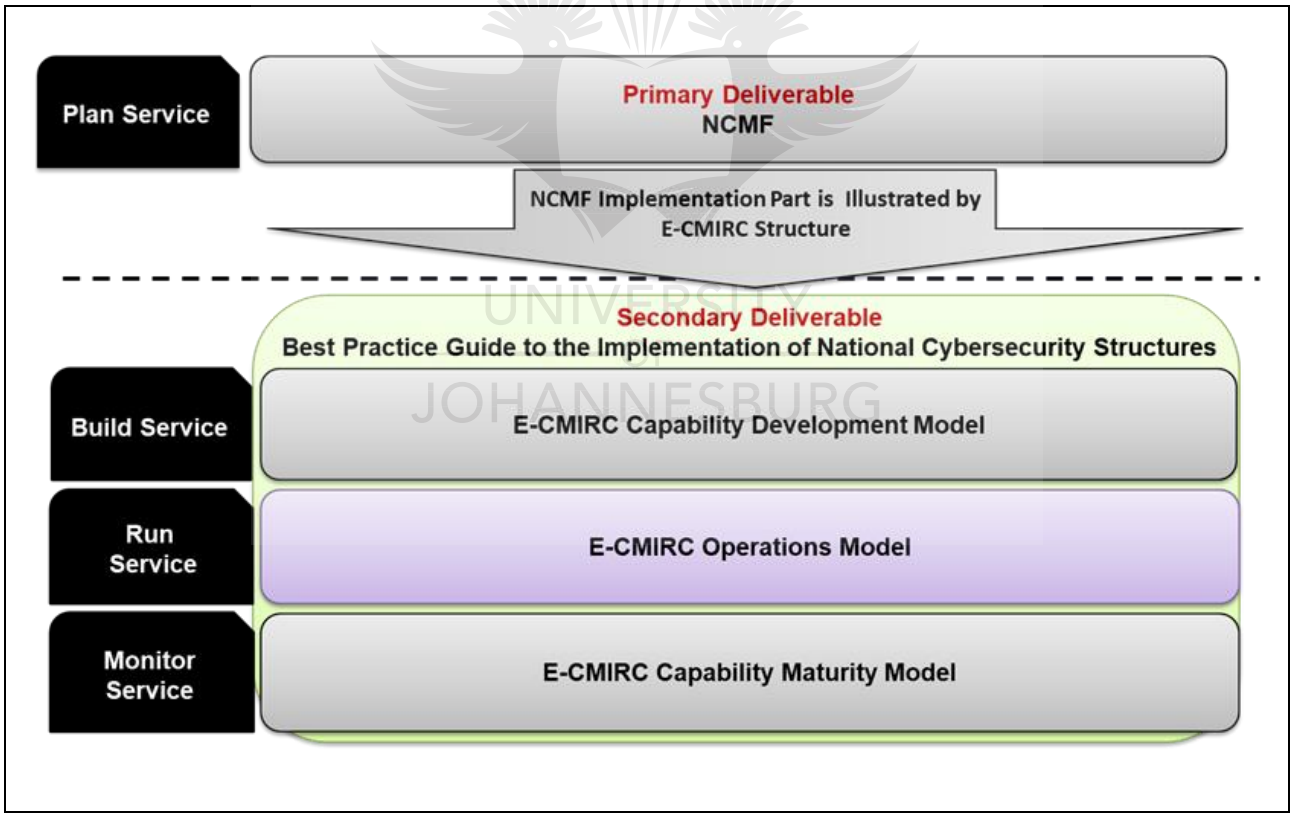



**Figure 6: Primary and secondary deliverables**

Figure 6 shows that the primary deliverable is the NCMF. The development of the NCMF satisfies the Plan function of the PBRM organisational approach in that the NCMF provides a framework that can be used to plan the execution of the cybersecurity management tasks. It further shows that the secondary deliverable is

a best practice guide that illustrates the implementation part of the NCMF. Our best practice guide will illustrate the implementation of a newly conceived national cybersecurity structure called the E-CMIRC. Three models describe the E-CMIRC structure. Once the national cybersecurity functions are identified, national cybersecurity structures are needed to offer those functions from.

## 1.10 Research design and methodology

We will be following three approaches during our research. The three approaches are:

- Conduct a thorough and comprehensive literature study.
- Develop an artefact, the NCMF.
- Illustrate the application of the NCMF's implementation part through the development of a best practice guide to implementing national cybersecurity structures. This guide will demonstrate the implementation of a newly conceived national cybersecurity structure called the E-CMIRC and is our second artefact.

This study will utilise the following research methodologies described next [17].

### 1.10.1 Theory building research

The research will focus on the availability of existing sources that are available for use during the identification, selection, prioritisation, and implementation of national cyber security functions, and applicable to developing countries. In terms of the E-CMIRC structure's models that will be developed as part of our best practice guide, research will be conducted on available models that can be used for the implementation of an early, or initial national cybersecurity structure in developing countries. From this research, the required elements for constructing a framework and a new structure, with descriptive models, will be identified.

### 1.10.2 Theory testing research

Applying this methodology, existing national cybersecurity functional prescripts, and its influencing elements will be identified from the sources identified during the theory-building research. This will provide a starting point for us to identify some of the function's complementary structures, with its services and technologies needed, to allow us to develop the E-CMIRC's models. In the absence of existing national cybersecurity prescripts that are applicable to developing countries, industry best practices, standards and frameworks will be identified and analysed to assist with the development of the initial or early national cyber defence monitoring and incident response structure.

### 1.10.3 Theory application research

We will then construct the framework and models that make up our best practice guide using the elements identified. The framework and E-CMIRC models will be developed using existing and proven publicly available frameworks, standards and best practices.

## 1.11 Structure of this thesis

The remainder of this study is structured according to the visual representation provided in Figure 7. This figure will be inserted at the beginning of every Chapter to contextualise our progress.

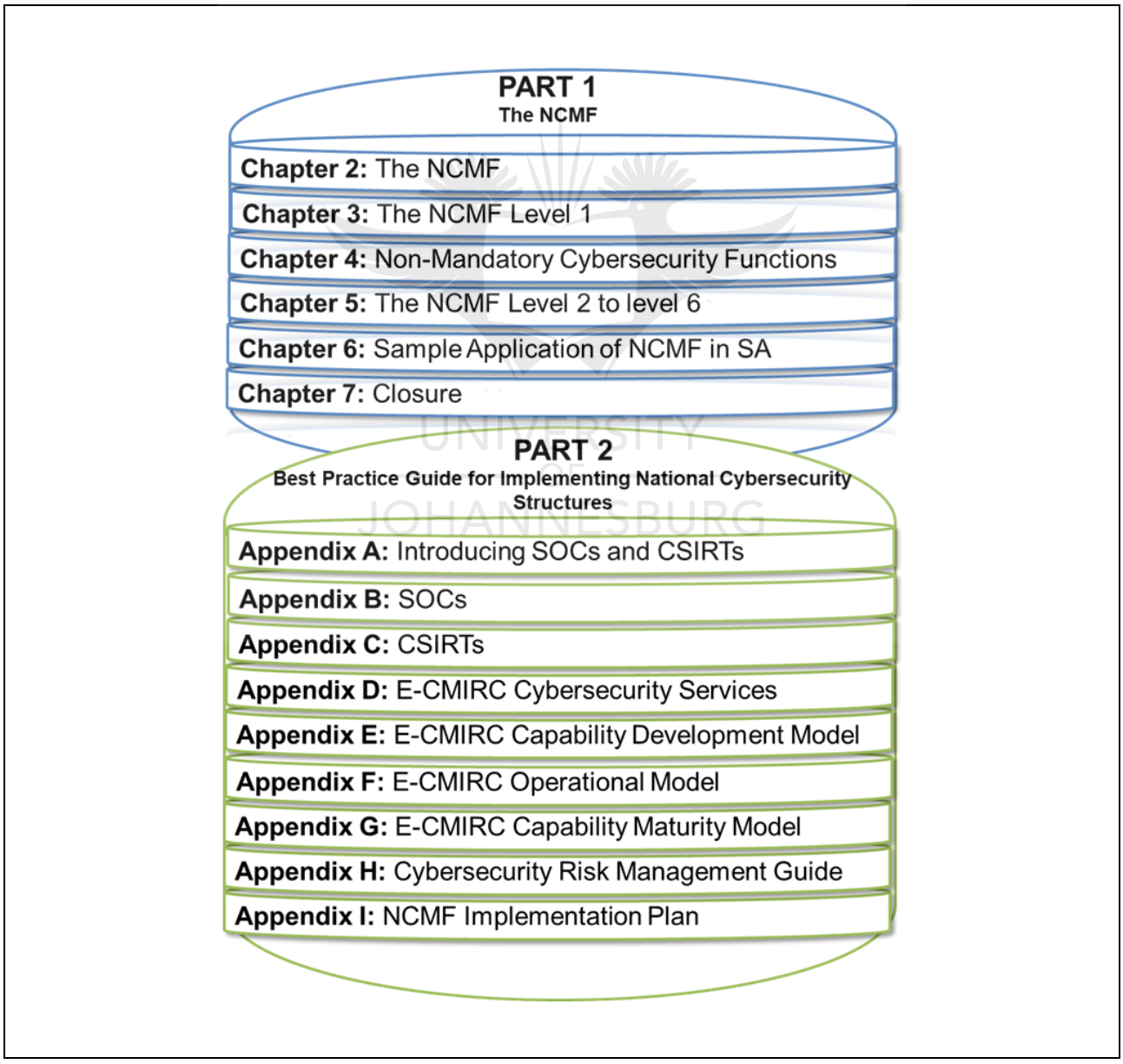



**Figure 7: Study roadmap**

Figure 7 shows that this study is divided into two parts. Part 1 covers the development of the NCMF. The NCMF satisfies the plan function of the PBMR organisational approach, and it will be used to identify, select and prioritise national cybersecurity functions. During the discussion of Part 1, we will apply the NCMF to identify some of the most general cybersecurity functions that are found across national and international authoritative and normative sources (describing non-mandatory and mandatory cybersecurity functions). We will then select two of these functions to be offered from a new structure.

Part 2 covers the development of our best practice guide that can be used during the implementation of national cybersecurity structures. Our best practice guide will demonstrate the implementation of a newly conceived national cybersecurity structure, the E-CMIRC. The E-CMIRC is described with three models, and in Appendix A, we propose a model to be used during the building of the structure from where the two selected general functions will be offered from. In Appendix B, we propose a model to be used during the running of the structure built in Appendix A. Appendix C covers the monitoring function, and we propose a model to monitor and improve the processes of the structure we have built.

**Part 1: NCMF**

In this thesis, we will focus, and spend more time on Part 1. Our motivation is as follows:

- Our aim, and primary deliverable is to develop a framework that can assist with cybersecurity management tasks at the national level.
- The framework satisfies the plan function of the PBMR organisational approach. Planning for the management of national cybersecurity functions is the first function to be completed, and is of paramount importance. We will develop a best practice guide to illustrate the implementation part of the NCMF. Our best practice guide will demonstrate the implementation of the E-CMIRC. This demonstration will be done through the development of three models describing the building, running and monitoring parts of the PBRM organisational approach. Nation states might however choose their own approach where it concerns the building, running and monitoring of cybersecurity structures. This is our secondary deliverable, and the best practice guide and E-CMIRC are not discussed in as much detail as the NCMF.

**Chapter 2 – The NCMF:** This chapter introduces and motivates the development of the NCMF. We introduce and define the terms “cybersecurity functions,” “services,” “capabilities” and “structures.” We illustrate some of the benefits to be gained by using a framework such as the NCMF, as well as the sources to be consulted by the NCMF during the identification of national cybersecurity functions. The NCMF is briefly introduced in this chapter.

**Chapter 3 – The NCMF Level 1:** Chapter 3 is dedicated to the development of level 1 of the NCMF. We start with a motivation for the existence of the NCMF's first level, as well as introducing authoritative and normative sources. Elements that could further influence the identification of national cybersecurity functions are identified and discussed. These elements are the dimensions, domains and mandates the NCMF could operate in. In Chapter 3, we also propose a stakeholder and actor identification template, as well as a domain function, structure and actor identification template to assist with the identification of national actors. Chapter 3 ends with a high-level introduction to general cybersecurity functions.

**Chapter 4 – General Cybersecurity Functions:** This chapter introduces and describes the general cybersecurity functions that we have identified using level 1 of the NCMF. Two of these functions will be selected, and their services and technologies combined to be offered from a newly envisioned national cybersecurity structure. This is done to illustrate the application of level 4 to level 6 of the NCMF.

**Chapter 5 – The NCMF Level 2 to Level 6:** Chapter 5 starts with motivating the existence of level 2 to level 6 of the NCMF. We then continue with the development of level 2 to level 6, with each level discussed individually.

**Chapter 6 – Sample application of the NCMF in South Africa:** Here we provide a sample application of the NCMF in the context of South Africa as a developing country. We end the chapter by proposing an implementation plan to be followed during the implementation of the NCMF.

**Chapter 7 – Closure:** This chapter provides an overview on the NCMF and maps the objectives to the outcomes. We will also be introducing our future work here.



**Part 2: National Cybersecurity Structure Best Practice Implementation Guide**

In this study, and during the development of our best practice guide, we will treat the E-CMIRC structure as a system. The development thereof could thus be done according to systems engineering (SE) principles, or by using an enterprise architecture (EA) approach. Whether an SE or EA approach is followed it depends on the outcomes we want to achieve. If the outcome is a new system, we will use SE principles. If the outcome is to integrate services, processes and technologies into existing services and processes, we will follow an EA approach. It is our experience that SE is useful in the development of specific technologies or systems, and EA is useful when developing and integrating new or existing cybersecurity services, processes and technologies into existing business processes.

Because we view the E-CMIRC as a system, we will follow SE principles to identify its functional requirements. An EA approach may be followed to integrate E-CMIRC services, processes and technologies after its establishment. In following an SE approach, the E-CMIRC structure's functional requirements will be identified, based on the national requirements of developing countries, and as expressed in prescripts found in legislation,

adopted standards and regulations. These national cybersecurity structure functional requirements are unique for each developing country.

**Appendix A – Introduction to SOCs and CSIRTs:** Appendix A introduces SOCs and CSIRTs at a high level. We are doing this to provide the reader with a better understanding of the SOC and CSIRT structures, functions, types and authority levels that follows in Appendices B and C.

**Appendix B – SOCs*:*** This appendix introduces the *monitoring and evaluation* function's structure. This structure is normally the security operations centre (SOC). The SOC is a most often a team of people, using specific technologies and processes to monitor for, and react to threats. We will introduce and identify the SOC's functions in this appendix.

**Appendix C – CSIRTs:** This appendix introduces the *incident handling* cybersecurity function's structure. The structure from where the *incident handling* cybersecurity function is offered from, is normally the Computer Security Incident Response Team (CSIRT). The CSIRT is a team of people using technology and processes to perform cybersecurity incident handling. The CSIRT functions are identified in this Appendix. The SOC and CSIRT functions are compared and similarities are identified. This provides us with a list of SOC and CSIRT functions. From this list, functions are selected for the E-CMIRC.

**Appendix D – E-CMIRC cybersecurity services:** This appendix identifies the complementary services of the E-CMIRC functions. Common and unique services and technologies are identified, and from these, some services are selected to be offered from the E-CMIRC structure.

**Appendix E – Build: E-CMIRC Capability Development Model:** The E-CMIRC CDM is developed in this Appendix. We introduce capability development models, and one model is selected, and its use for the development of the E-CMIRC CDM is motivated. The E-CMIRC CDM and E-CMIRC OM are presented as a single model.

**Appendix F – Run: E-CMIRC Operations Model:** In this appendix, the E-CMIRC Operations Model is developed. The available operational models are introduced, and one model is selected and motivated for use in the development of the E-CMIRC OM. The rationale for presenting the E-CMIRC CDM and OM as a single model is that E-CMIRC services will be prescriptive regarding the capability development requirements, which in turn influences the operations model.

**Appendix G – Monitor: E-CMIRC Capability Maturity Model:** We will develop the E-CMIRC Capability Maturity Model in this appendix. This appendix introduces available capability maturity models, and one is selected and motivated for use in the development of the E-CMIRC CMM.

**Appendix H – National Cybersecurity Risk Management Guide:** This appendix proposes a national cybersecurity risk management guide. This guide may be useful for nation states that do not have an existing national cybersecurity risk management strategy and process. The intention is for our national cybersecurity risk management guide to be used to select and prioritise national cybersecurity functions for implementation.

**Appendix I – NCMF implementation plan for South Africa:** In this appendix, we propose a plan on how to implement the NCMF in South Africa. We also provide critical success factors to consider when implementing the NCMF.

## 1.12 Research output

In this section, we introduce our research output at the point of submission. The focus of our past research had mainly been on SOCs and the development of SOC models. Research not directly related to this study contributed in terms of the knowledge we have gained on frameworks and models, as well as operational aspects of security management.

### 1.12.1 Articles and presentations by the author directly related to this study

Our study resulted in the articles and presentations listed below. The knowledge gained during this research was used in the writing of this thesis, and we also used it as a mechanism to validate our models with peers. These articles influenced our thesis, and valuable knowledge was gained in terms of SOC and CSIRT functions, as well as the development of frameworks and models. The articles below is a direct result of this study.



**1. Framework for the implementation of business cybersecurity**

| | |
|---|---|
| **Author(s):** | PC Jacobs (Presenter), MM Grobler, SH von Solms |
| **Date:** | 12 - 13 May 2016 |
| **Type:** | **Conference**<br>London, United Kingdom: International conference on Business and Cyber Security (ICBCS)<br>Article:<br>(https://www.researchgate.net/publication/305769629_Towards_a_framework_for_the_development_of_business_cybersecurity_capabilities) |
| **DOI:** | 10.13140/RG.2.1.5110.0406 |
| **Relevance** | **Chapter 2 and 4:** This article applied the NCMF in an organisational environment, thus demonstrating its breadth and flexibility. |
| **Abstract** | 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 cyber domain. 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.

**2. E-CMIRC – Towards a model for the integration of services between SOCs and CSIRTs**

**Author(s):** PC Jacobs (presenter), SH von Solms, MM Grobler
**Date:** 25 – 26 July 2016

**Type:** **Conference**

Munich, Germany: 15th European Conference on Cyber Warfare and Security (ECCWS-2016) (Refereed and Published)

**DOI:** 978-1-910810-96-5

**Relevance** **Appendix D:** This article presented an integrated services model for SOCs and CSIRTs. This knowledge was used during the identification and selection of services to be offered from the E-CMIRC.

**Abstract** Security Operation Centres (SOCs) and Computer Security Incident Response Teams (CSIRTs) or Computer Emergency Response Teams (CERTs) can play a pivotal role in the monitoring of, and response to threats, attacks and vulnerabilities in organisations, including governments. While the focus of a SOC is on the monitoring of technical security controls and critical assets, and the response to attacks and threats, CSIRTs' main focus is on response and incident management. One postulation is that a CSIRT or CERT is a highly specialised sub-capability of a SOC, whereas another postulation could be that a SOC serves as an input mechanism into CSIRTs and CERTs. In this paper, the differences between SOCs, CERTs and CSIRTs are established, and synergies between them are defined. This leads to an

integrated services model for the establishment of an initial SOC and CSIRT capability in developing countries. Developing countries have unique challenges facing them where it concerns cybersecurity. Aspects such as Information Communication and Technology (ICT) Infrastructure is often a challenge, and so is funding for ICT as well as skills. Political instability could also influence the cybersecurity posture of developing countries by leaving developing nations open to malicious state-sponsored attacks. This SOC and CSIRT capability are made viable and possible through the savings in cost and resources by identifying overlapping services, as well as the application of the proposed model. This emergent SOC and CSIRT combined capability is called the Embryonic Cyberdefense Monitoring and Incident Response Centre (E-CMIRC). The purpose of this paper is to identify a high-level integrated services model for the E-CMIRC in order to reduce cost and resources which serves as a barrier to entry in developing countries. A scalable operational framework is identified, and for the management of the effectiveness and efficiency, and also to ensure that all aspects of service delivery are considered, the Information Technology Information Library (ITIL) is proposed.

## 3. Towards a National Cybersecurity Capability Development Model

**Author(s):** PC Jacobs (presenter), SH von Solms, MM Grobler

**Date:** 28 – 30 July 2017

**Type:** **Conference**

Dublin, Ireland: 16th European Conference on Cyber Warfare and Security (ECCWS) 2017 (Refereed and Published)

**ISBN:** 2048-8602

**Relevance** **Appendix E**: The knowledge gained with this article was applied during the development of the E-CMIRC CDM.



**Abstract** Nations need to develop cybersecurity capabilities at the national level in order to facilitate the requirements expressed through national authoritative and normative documents. These national cybersecurity capabilities typically consist of people, processes and technology or tools. From the research conducted, no publicly available models or frameworks for national cybersecurity capability development could be found. In this paper, the authors identify and compare existing military capability development models and propose a national cybersecurity capability development model based on these models. Military capability development frameworks are a comprehensive way to define work deliverables and work standards and provides a way to measure the work deliverables (eWorks Moodle, 2016). The use of such a national cybersecurity capability development model is advantageous during the planning phase of the national cybersecurity capability. For example, the using of a model allows for a capability to be broken down into its components; a model serves as a blueprint to ensure that those building the capability considers all components, allows for cost estimation and facilitates the evaluation of trade-offs. One national cybersecurity capability –

the incident management cybersecurity capability - is selected to illustrate the application of the national cybersecurity capability development model.

This model was developed as part of previous research and is called the Embryonic Cyberdefence Monitoring and Incident Response Centre (E-CMIRC) (P. Jacobs; S.H. von Solms & M.M. Grobler, 2016). The characteristics of national incident management cybersecurity incidents have to be determined, as these would affect each component of the military-based national cybersecurity capability development model. Once the national cybersecurity capability components are identified using the military-based cybersecurity capability development model, it also has to be operated. To achieve this requirement, available organisational, operational models are identified and compared, and one operating model is selected to augment the national cybersecurity capability development model. The fusion of the military-based national cybersecurity capability development model with the operations models results in the national military-based cybersecurity capability development model. This paper has three outcomes in mind: firstly, to determine the characteristics of national cybersecurity incidents, secondly, the development of the national cybersecurity capability development model, and thirdly, the development of a national cybersecurity capability operational model. This paper describes the methodology followed in describing the E-CMIRC structure using a capability development framework, and organisational, operational models. The national cybersecurity capability development model – using a military capability development framework - and the national cybersecurity capability operational models derived from existing organisational frameworks, are presented as a single, integrated model.



## 1.12.2 Articles and presentations by the author relevant to this study

The articles and presentations below is not a direct result of this study, but the knowledge gained here was used during the writing of this thesis.

**4. Classification of security operations centres**

| | |
|---|---|
| **Author(s):** | PC Jacobs (Presenter); A Arnab; B Irwin |
| **Date:** | 14-16 August 2013 |
| **Type:** | **Conference** |
| | Pretoria, South Africa |
| | Article |
| **DOI:** | 978-1-4799-0808-0 |

**Relevance** **Appendix G:** *Monitoring and evaluation* function: This article identified SOC functions and services, and proposed a framework to be used for classifying SOCs. This information is used in Appendix G.

**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 address the technology aspects of these services, a holistic framework addressing processes, staffing and technology currently do not exist. Additionally, it would be useful for organisations 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.

## 5. Towards a Secure Datacenter Model

**Author(s):** PC Jacobs; B van Niekerk

**Date:** 01 August 2015

**Type:** **Journal Article**
**ISACA Journal Volume 3**
Article: (https://www.isaca.org/Journal/archives/2015/Volume-3/Documents/Toward-a-Secure-Data-Center-Model_joa_Eng_0515.pdf)

**ISSN:** 1944-1967

**Relevance** **Appendix E, F and G**: The knowledge we gained in developing models is applied in Appendix E, F and G. during the development of the E-CMIRC models.

**Abstract** According to a survey by Infonetics Research, companies operating their own data centres spent an average of US $17 million on security products in 2013. The top drivers, according to respondents, were the need to protect virtualised servers, upgrade security products to match network performance and obtain new threat protection technologies. Most modern data centres use virtualised servers. This technology allows multiple servers to run on a single hardware instance. The fact that all server instances, as well as databases, are now flat files dramatically increases the attack vector. It also opens up additional avenues of attack that could not be used in normal data centres (such as dark virtual machines [VMs] and VM sprawl). It is also true that virtualisation drives cloud, and cloud, in turn, enables and drives mobility. This has unique challenges in a military environment or high-security organisational setting where the security requirements are more stringent than those in the majority of organizations in the private sector.

While this article focuses on military-grade data centres, this does not exclude corporate data centres. For certain projects, defence contractors are required to maintain military-grade security for data centres relevant to the project. Many other corporate entities that handle

sensitive or critical information or services may also choose to implement military-grade security in their data centres. Such entities may include financial companies and critical infrastructure providers such as telecommunications or power companies. Pharmaceutical companies that conduct research and development can benefit from implementing military-grade data centre security to protect their intellectual property. Many of these types of companies are targeted by cyberespionage campaigns using advanced persistent threats (APTs)

### 6. Cloud-based security mechanisms for critical information infrastructure protection

**Author(s):** B van Niekerk (Presenter); PC Jacobs

**Date:** 25-27 November. 2015

**Type:** **Conference**

Pretoria, South Africa: 2013 International Conference on Adaptive Science and Article (Published).

**ISBN:** 978-1-4799-3067-8

**Relevance** **Chapter 4, Appendix B, C and D:** The article presented cloud-based monitoring and incident handling function. The knowledge gained here was applied in Chapter 4 during the identification of national cybersecurity functions, as well as the identification of the services supporting the *incident handling function* and *monitoring and evaluate* function.

**Abstract** In this paper, the suitability of cloud-based security services (SECaaS) for critical information infrastructure protection (CIIP) is discussed. A background of cloud-based security services is provided. The suitability of these services for CIIP is discussed, and it is concluded that a mixed cloud and traditional solution is best. A model for providing cloud-based protection to critical infrastructure in this manner is proposed.

### 7. SOCs and CSIRTs - a view from a SAPS perspective

**Author(s):** PC Jacobs (presenter)

**Date:** 16 January 2016

**Type:** **Conference**

Irene, Centurion: South African Police Service (Hawks) Cybercrime Conference Presentation

**TOdB Pub number:** (TOdB Pub number: CSIR/DPSS/ISG/EXP/2015/0102/A)

**Relevance** **Appendix D**: The knowledge gained here was used during the identification of SOC and CSIRT services in Appendix D.

**Abstract** 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. We present

a model to measure the effectiveness and capabilities of a SOC, through three aspects. These are the functional requirements of SOC services; the measures of effectiveness of functional requirements; and the maturity of SOC functional requirements.

**8. Threat mitigation and detection of cyber warfare and terrorism activities**

| | |
|---|---|
| **Author(s):** | MM Grobler, PC Jacobs, B van Niekerk |
| **Date:** | 28 – 30 July 2017 |
| **Type:** | Chapter 2 p 21 - 51: Cyber Security Centres for Threat Detection and Mitigation |
| **DOI:** | 10.4018/978-1-5225-1938-6 |
| **ISBN:** | 9781522519386 |
| **Relevance** | **Appendix B to G:** The knowledge gained during the writing of his book chapter was applied during the identification of monitoring and incident handling services at national level, and during the development of the E-CMIRC reference models. |
| **Abstract** | Technology provides numerous opportunities for positive developments in modern society; however, these venues inevitably increase vulnerability to threats in online environments. Addressing issues of security in the cyber realm is increasingly relevant and critical to society. Threat Mitigation and Detection of Cyber Warfare and Terrorism Activities is a comprehensive reference source for the latest scholarly perspectives on countermeasures and related methods to enhance security and protection against criminal activities online. Highlighting a range of topics relevant to secure computing, such as parameter tampering, surveillance and control, and digital protests, this book is ideally designed for academics, researchers, graduate students, professionals, and practitioners actively involved in the expanding field of cyber security. |



## 1.13 Conclusion

Developing countries face unique challenges where it concerns their national cybersecurity function management tasks. Some of these challenges are a lack of skills, and not enough fiscal resources. During a comprehensive literature survey, no framework to assist with the national cybersecurity management tasks of identification, selection, prioritisation and implementation of national cybersecurity functions, could be identified. In this study, a conceptual Framework is developed to assist with the management tasks associated with national cybersecurity functions. The Framework is the NCMF, and it satisfies the plan function of the PBRM organisational approach. This Framework will be developed in Part 1.

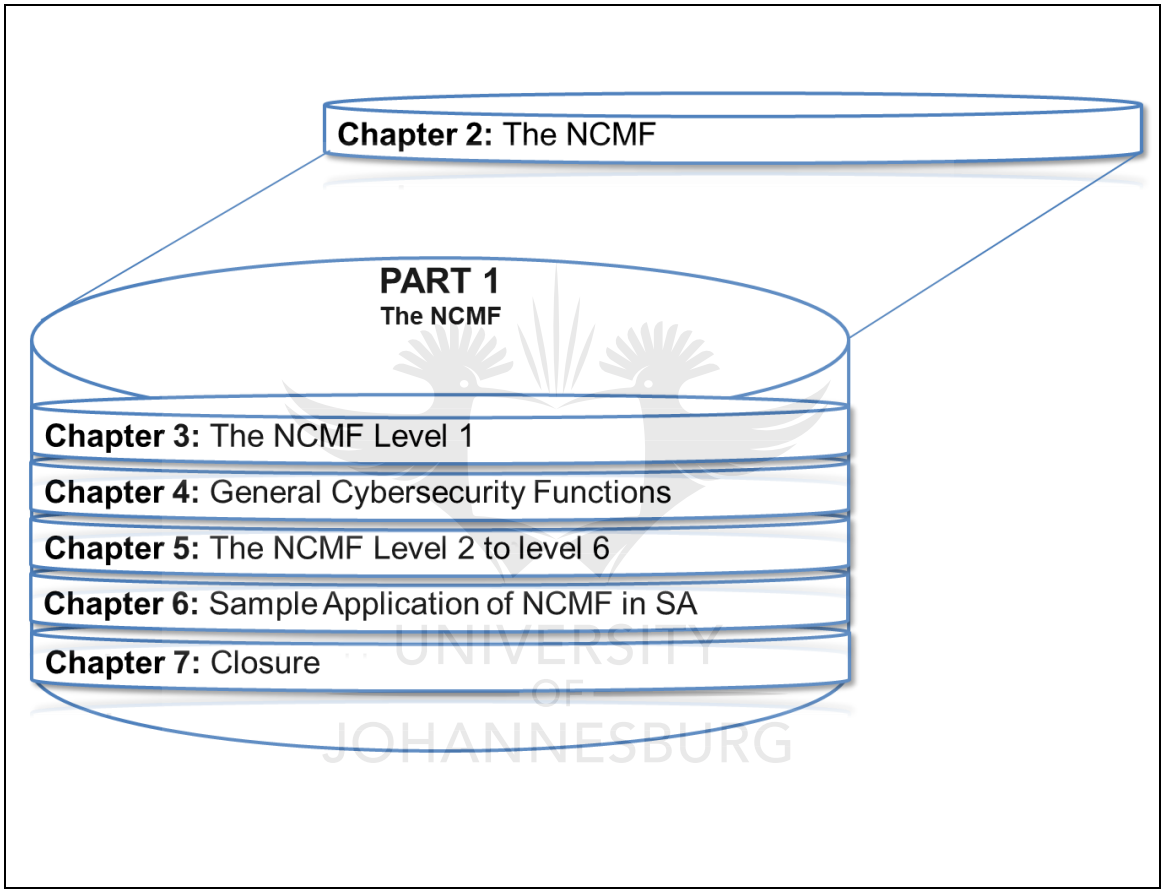
In this thesis, the framework process to identify nation state mandatory cybersecurity functions that are specific and applicable to nation states in nature, as well as general cybersecurity functions that are non-mandatory in nature is explained. The NCMF will then be applied to identify the most general cybersecurity functions from

national and international authoritative and normative sources (describing non-mandatory and mandatory cybersecurity functions). To illustrate the implementation part of the NCMF, a new national cybersecurity structure is envisioned to offer some of the identified general cybersecurity functions.

From the identified general cybersecurity functions, we will select two, and their services and technologies are merged. A single, new national cybersecurity structure is developed from where the merged services are being offered. This new national cybersecurity structure is called the E-CMIRC. The E-CMIRC is developed in Part 2.

The building, running and monitoring of the E-CMIRC will be described through the development of three reference models. These are the E-CMIRC Capability Development Model, the E-CMIRC Operations Model and the E-CMIRC Capability Maturity Model. These three models satisfy the build, run and monitor functions of the PBMR organisational approach.

Chapter 2 introduces the NCMF at a high level. The NCMF will be used as a guide during the national cybersecurity function management tasks of identification selection, prioritisation, and implementation of national cybersecurity functions.



# Chapter 2: The National Cybersecurity Management Framework (NCMF)

## 2.1 Introduction

The main objective of Chapter 2 is to provide a high-level introduction of the NCMF. The aim is to aid the reader to obtain a better understanding the detailed discussion of the NCMF in the following Chapters. The NCMF is a layered framework, consisting of six sequential levels. Due to its foundational nature, level 1 is introduced and discussed in detail in its own Chapter - Chapter 3, while level 2 to level 6 are introduced and discussed in Chapter 5.

This chapter will introduce a high-level organisational framework that we will use to guide us during the development of the NCMF. To understand the NCMF, it is important to have an understanding of the terminology used during its development, such as functions, services, capabilities and structures. The statement was made in Section 1.3 that the NCMF is developed as a framework to manage national cybersecurity functions, and that there are four tasks associated with the management of national cybersecurity functions. These four tasks are the:

- **Task 1:** Identification,
- **Task 2:** Selection,
- **Task 3:** Prioritisation, and,
- **Task 4:** Implementation of national cybersecurity functions.



It will be explained in Section 2.4 that national cybersecurity functions consist of services, and that these services are made up of capabilities. The services realising these functions are offered from national cybersecurity structures. It is thus necessary to have a good understanding, and a common definition of the terms “cybersecurity functions”, “cybersecurity services” and “cybersecurity capabilities” before introducing the high-level overview of the NCMF. Chapter 2 starts by motivating the development of an NCMF, and then introduce, and define the terms cybersecurity functions”, “cybersecurity services” and “cybersecurity capabilities” since an understanding of these terms is key to the understanding the NCMF. Chapter 2 is structured as follows:

**Section 2.2** - This section provides a motivation for the development of an NCMF.

**Section 2.3** - Introduces and motivates our high-level organisational framework for use during the development of the NCMF.

**Section 2.4** - This section introduces and defines the terms cybersecurity function, cybersecurity service and cybersecurity capabilities to foster a common understanding of the framework terms, and its elements.

**Section 2.5** - Contextualises functions, services and capabilities for South Africa as a developing country.

**Section 2.6** - This section provides background information on frameworks in general, and the benefits realised by using them. The terms authoritative and normative sources are also introduced in this section. These sources contain important national and international cybersecurity prescripts, and they serve as the primary source from where mandatory national cybersecurity functions are identified from.

**Section 2.7** - Introduces and advances the understanding of mandatory and non-mandatory cybersecurity functions.

**Section 2.8** - Introduces elements such as dimensions, mandates and domains that may influence the NCMF, and the identification, selection and prioritisation of national cybersecurity functions.

**Section 2.9** - This section introduces the six levels of the NCMF, and it provides a high-level overview of each of the six levels. The NCMF's six levels are mapped back to the four national cybersecurity management tasks of the NCMF.



**Section 2.10** - Provides an overview of the differences between NCMF levels 5 and 6 prescripts.

**Section 2.11** - Provides a mapping of the NCMF levels to its explicit functions.

**Section 2.12** - Concludes this chapter.

Section 2.2 will provide a motivation for the development of the NCMF. The term "framework" is defined, and we then highlight some of the benefits realised by using a framework during the identification of national cybersecurity functions.

## 2.2 Motivation for the development of an NCMF

In Section 1.3 the necessity for a ***N**ational **C**ybersecurity **M**anagement **F**ramework* (NCMF) was motivated. Such a framework can assist to guide and steer both developed and developing

countries during the cybersecurity management tasks of identifying, selecting, prioritising, and implementing cybersecurity functions.

The Oxford dictionary defines a framework as *"a set of beliefs, ideas or rules that are used as the basis for making judgements, decisions, etc."* [18]. A frameworks is intended to be used as a reference when planning or building something [19]. Frameworks do not provide instructions on *how* to plan or develop something, but it serves as *guidance* during the planning and development process. Accordingly, frameworks should be flexible and fluid in terms of situational requirements [19].

Using an NCMF to assist with the cybersecurity management tasks reduces costs, in that only applicable and relevant national cybersecurity functions are selected for implementation. The use of an NCMF will also lead to repeatable, consistent and sustainable results when implementing national cybersecurity functions. Advantages of using a framework such as the NCMF are that it [19]:

- Provides a mechanism to consider - and align with - all relevant national legislation and regulations when identifying national cybersecurity functions.
- Allows for the consideration of national and international ICT security and cybersecurity best practices and allow for the maximisation of the strengths of each where appropriate.
- Provides a mechanism for nation states to demonstrate their security efforts, and in the process, foster trust between trade partners.
- Ensures a consistent experience for the population interacting with national cybersecurity functions and structures.
- Promotes consistent service delivery from national cybersecurity structures to the population.
- Provides a common language when referencing aspects of the cybersecurity function under planning, or during implementation.
- Allows repeatable and consistent delivery and outcome of the cybersecurity functions during implementation.
- Promotes predictable budgeting.

Now that we have discussed the benefits to be gained by using an NCMF, we will discuss and select a high-level organisational approach to guide us during the development of the NCMF.

## 2.3 Selecting a high-level organisational approach

An organisational structure is usually associated with how the lines of authority, duties and channels of communication within an organisation are arranged. It determines the assignment of roles and

responsibilities, and also coordination and control structures. The organisational structure is influenced by the organisation's strategy and objectives [20]. Structuring an organisation thus provides stakeholders with different perspectives to view their organisation from [21].

Organisational structures help to define the parameters that are needed at government or organisational level to achieve the organisation or national objectives. A high-level organisational approach should describe the distribution of authority, the assignment of responsibility and departmental involvement that is needed during the development and national implementation of cybersecurity functions. This high-level organisational approach should also prioritise the tasks needed to realise an end-goal, and determine the tasks ranking [22].

Using an organisational approach based on technology when developing national IT systems has limitations in terms of scalability, changes in technology, innovation, and expectations of stakeholders. It is, therefore, preferable to use an organisational approach based on functions. Using a functional instead of a technological approach addresses the limitations of following a technological approach. Such a functional approach is the Plan-Build-Run-Monitor approach [23].

The build function of the plan-build-run-monitor approach describes the technology and resources needed to build structures, and we will use the Build function to describe a national cybersecurity structure. The run function of the plan-build-run-monitor approach describes the operation and management of structures, and we will be using the build function to describe the operation and management of a national cybersecurity structure. Both the build and run functions may be described with a model, and due to the overlap between some structure's technology and resources (build function), and its supportive processes and procedures (run function), it is possible to describe them using a single, integrated model.



The monitor function of the plan-build-run-monitor approach describes the continuous monitoring and improvement of structures such as national cybersecurity structures. We will be using the monitor function to describe the continuous monitoring and improvement of a national cybersecurity structure. This function may also be described with a model [24].

To achieve the advantages mentioned in Section 2.2, and after our description of the PBRM organisational approach in Section 2.3, it is important to now foster a common understanding of the terms cybersecurity functions, services and capabilities. This allows the reader to accurately understand and interpret the intention and meaning of the terms as they are used throughout the thesis. This needs to be done early, and before introducing the NCMF in detail. Therefore, Section 2.4 defines cybersecurity functions, services and capabilities. These concepts are pivotal to understanding and interpreting the NCMF.

## 2.4 Defining cybersecurity functions, services and capabilities

In this section, the terms “cybersecurity functions,” “cybersecurity services,” “cybersecurity capabilities” and “cybersecurity structures” are introduced and defined. To foster a common understanding, and to avoid ambiguity in the interpretation of the terms functions, services, capabilities and structures, these terms are now defined.

### 2.4.1 Cybersecurity functions

A function describes work or operations that must be performed to achieve a mission, or accomplish a national responsibility [25], [26]. The Merriam-Webster dictionary defines a function as “the action for which a person or thing is specially fitted or used or for which a thing exists” [27]. BusinessDictionary defines a function as "an action performed by a device, department, or person that produces a result. Function remains more or less fixed whereas the purpose (which indicates intention or objective) generally changes." [28] Synonyms for the meaning of the word “function”, is “objective” or “purpose” [29].

Using a SOC as an example, one of a SOCs functions is to monitor for threats and vulnerabilities. For the purpose of this study, and to create a common understanding, the term national cybersecurity function is defined as follows to ensure a constant interpretation, and to prevent ambiguity when referring to the term cybersecurity function:



**National cybersecurity function**

A national cybersecurity function describes work to be performed by governments, and their responsibilities in securing the national cyberspace. National cybersecurity functions are enabled through national cybersecurity services.

### 2.4.2 Cybersecurity services

Considering the definition of a national cybersecurity function, we see that national cybersecurity functions are realised through cybersecurity services. Our understanding is supported by Graves [7]. The cybersecurity services are offered from national cybersecurity structures. A service describes work that supports functions. Services thus realise functions. National cybersecurity functions consist of national cybersecurity services.

In keeping with using a SOC as an example, some of the services provided by a SOC in support of the monitoring function, is the monitoring and review the logs of security controls, or to review

sources for threat intelligence, and then to report on this information. In the development of the NCMF, and during its implementation, the term national cybersecurity service is defined as follows:

**National cybersecurity service**

A national cybersecurity service is work performed at national level to enable a national cybersecurity function. Cybersecurity services are intangible, and can be described as a valuable effort or action that satisfies a function, need or demand. National cybersecurity services consist of capabilities.

### 2.4.3 Cybersecurity capabilities

At a more granular level, a service consists of capabilities [7]. Capabilities, in turn, are made up of people, processes and technology [30]. The Merriam-Webster dictionary defines a capability as "the facility or potential for an indicated use or deployment" [31] while the Systems Engineering Body of Knowledge (SEBoK) defines a capability as "a range of systems, processes, people, information and organizations." [32]. A capability refers to the ability of a system or structure to perform certain actions, and achieve specific outcomes. The SOC monitoring and reporting services thus consist of the people (SOC engineers), technology (the technology most commonly found in a SOC is the security incident and event monitoring technology) and processes (the monitoring and reporting process). The following definition is provided to ensure a common understanding of the term cybersecurity capability.



**National cybersecurity capability**

A national cybersecurity capability refers to the achievement of specific actions and outcomes in the cybersecurity domain. National cybersecurity capabilities support national cybersecurity services. A national cybersecurity capability consists of people, processes and tools or technology[6], and is performed from a system or structure.

## 2.5 Contextualising functions, services and capabilities

Figure 8, as taken from Graves [7], illustrates that a function is realised through services. It shows further that service consists of capabilities, and that a capability is made up of people, processes and technology. The coloured arrows show that there exist flow and exchanges between services. The national cybersecurity functions will thus require services to fulfil them. In order to provide these

[6] The term "capabilities" from hereon should be understood to include people, processes and technology.

national cybersecurity services, its complementary capabilities need to be developed or implemented.

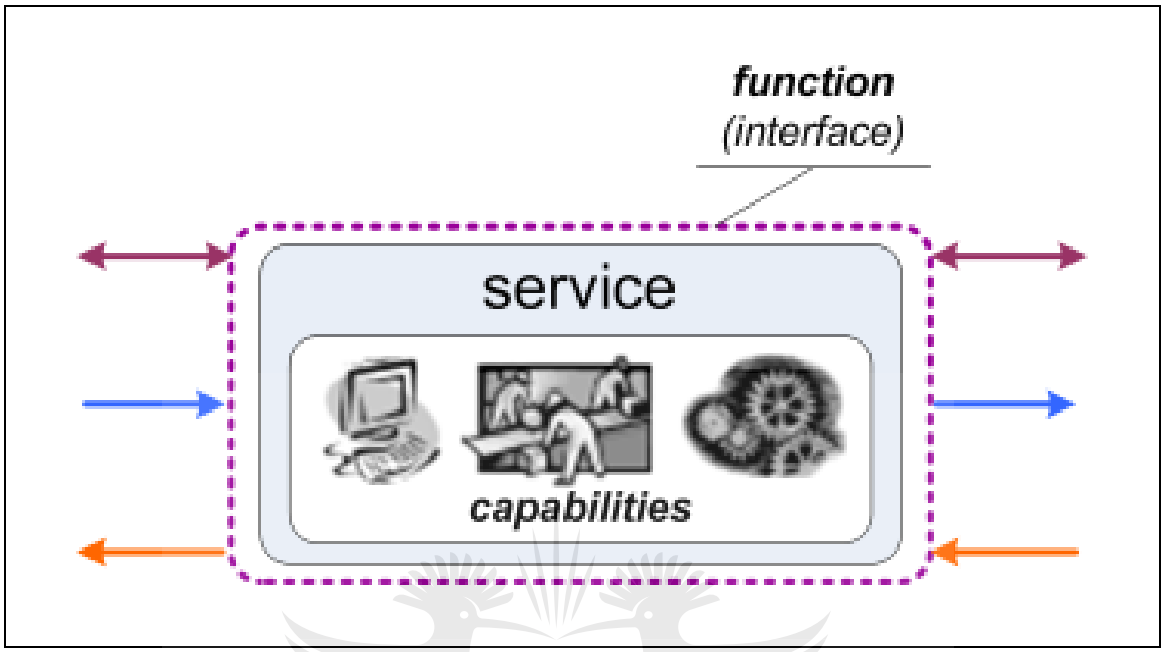



**Figure 8: Relationship between service, function and capability** [7]

Figure 9, which repeats Figure 3, contextualises cybersecurity functions, services, capabilities and structures. Figure 9 shows that national cybersecurity functions consist of national cybersecurity services that are made up of cybersecurity capabilities. National cybersecurity functions are offered from national cybersecurity structures.

We will illustrate Figure 9 in the context of South Africa. The South African National Cybersecurity Policy Framework (NCPF) [6] prescribes the establishment of a South African national cybersecurity incident handling function. This national incident handling function is enabled through the implementation of national cybersecurity services. To contextualise this statement, the national incident handling function may be enabled by an incident management service and an incident escalation service.

The incident management and incident escalation services consist of capabilities, such as the incident management capability. The incident management capability consists of people, or staff managing and acting on the incident (people). They will follow a process, such as a defined incident management process (processes). The incident management process is captured by, or the investigation thereof enabled by helpdesk or incident management software (tools or technology).

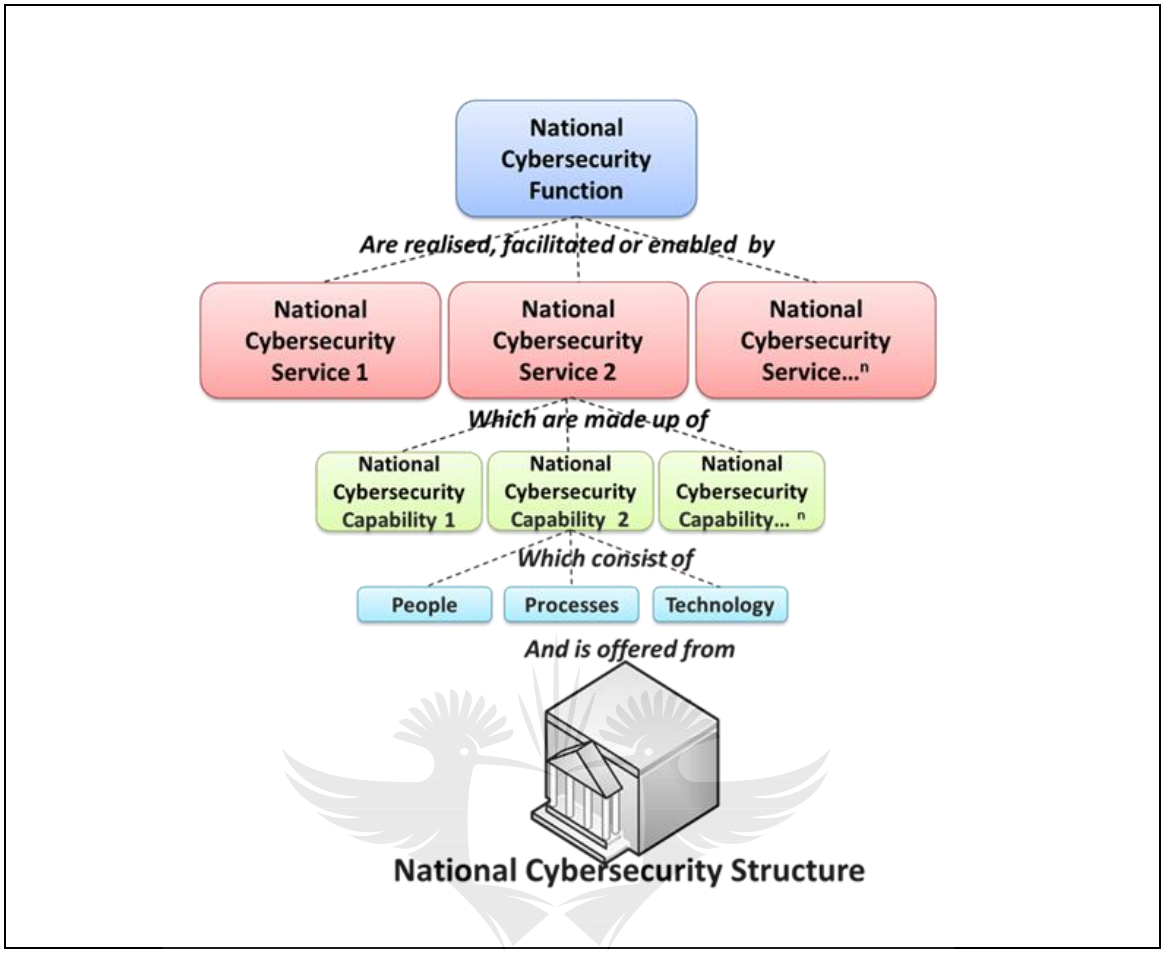



**Figure 9: Relationship: Functions, services, capabilities and structures (Figure 1 repeated)** [7]



Our discussion of the national incident handling function with its services and capabilities is illustrated in Figure 10 that shows that the national incident handling function may consist of two services, the incident management service, and the incident escalation service. These two services, in turn, consist of capabilities that are made up of people, processes and technologies.

The two services may make use of the same, or similar technologies. They may also have similar or overlapping processes. These similar technologies and overlapping processes may then be combined to realise a cost benefit. As an example, Figure 10 shows that the incident management service may use a technology called the “incident management software”. This software may provide functionality that can also deliver on the Incident Escalation Service. Furthermore, the incident management process and the incident escalation process may have overlaps in terms of sub-processes or steps.

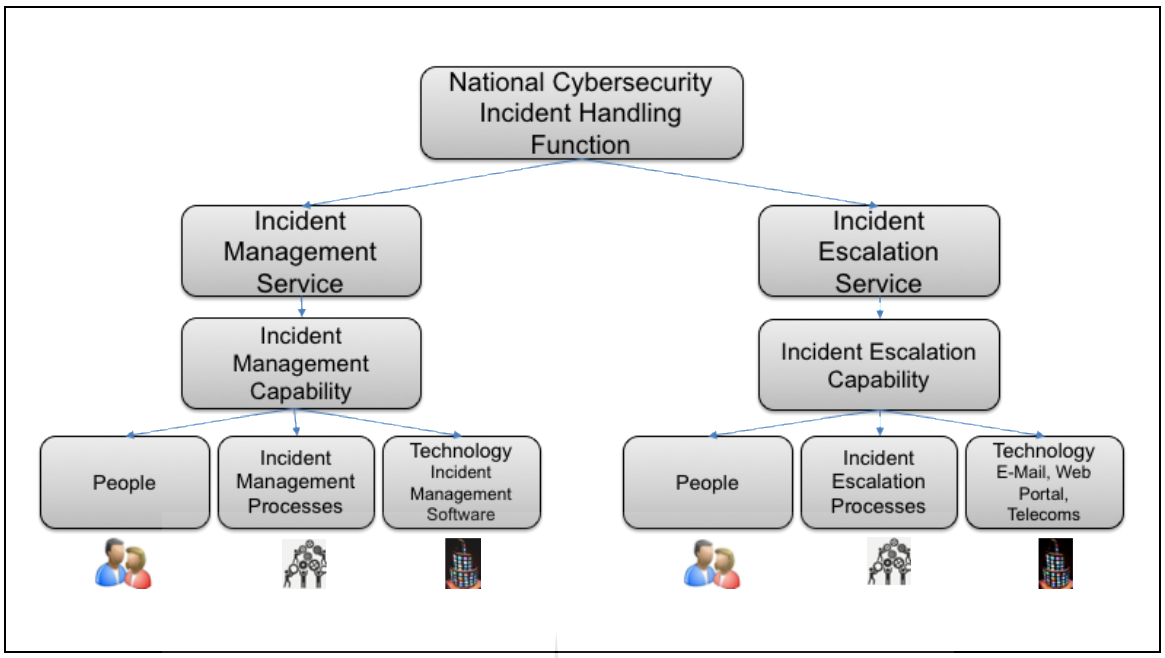



**Figure 10: National Incident Handling Function, Services and Capabilities**

Section 2.6 provides background to the NCMF, and it introduces the concepts of 'national and international authoritative and normative sources'. These sources are important in that they provide mandatory prescripts and recommendations for cybersecurity functions.

## 2.6 Authoritative and normative sources related to the NCMF

It is our experience that any national framework must have a starting point or a foundation from where elements influencing the framework are identified. We have experienced that in the development of a framework at the national level, and applicable to national cybersecurity, some considerations need to be taken into account. One of the considerations is that it must operate within the ambit of the nation state's legal and regulatory structure and that it must consider the prescripts described in the national legal and regulatory structure.

Sources that prescribe mandatory national cybersecurity functions are called authoritative sources. Some sources only make recommendations, and these are called normative sources. It is important though to understand that authoritative sources *prescribe* mandatory national cybersecurity functions, and the normative sources *recommend* general cybersecurity functions. Mandatory functions *have* to be implemented. Failing to implement them could lead to sanctions, such as fines, audit findings or expulsion from international bodies. General cybersecurity functions that are Non-mandatory in nature, *may* be implemented, and no sanctions are associated with not implementing them.

Authoritative sources thus *prescribe*, (mandatory) and normative sources r*ecommend* general cybersecurity functions that are non-mandatory in nature.

We will thus consult two types of sources. The two types of sources are:

- National authoritative and normative sources - describing national mandatory and non-mandatory cybersecurity functions.
- International authoritative and normative sources - describing international mandatory and non-mandatory cybersecurity functions.

These two types of sources provide us with two categories of cybersecurity functions. The first category is mandatory national cybersecurity functions that are specific to a nation state, and the second category is general cybersecurity functions that are non-mandatory in nature. These two categories are discussed in more detail in the text following.

- Nation-state mandatory, specific and applicable national cybersecurity functions are identified form national and international authoritative sources. Nation states have the option to augment their specific and mandatory national cybersecurity functions with the general (non-mandatory) cybersecurity functions. Since we have experience working on South African national cybersecurity efforts, only South African mandatory functions described in South African authoritative sources will be considered in this thesis.

- The general cybersecurity functions that are non-mandatory in nature, are identified from national and international normative and authoritative sources provide nation states with a pre-defined list of cybersecurity functions that are general in nature, and from which they may select one, or many from, for implementation. General cybersecurity functions are by definition non-mandatory.

A nation-state without its own authoritative sources may make use of a different country's authoritative source documents, and from there, identify general cybersecurity functions for itself. Normative sources are documents such as standards, frameworks and best practices. Mandatory and general cybersecurity functions are discussed in more detail in the following sub-sections.

### 2.6.1 Mandatory cybersecurity functions

The sources providing mandatory prescripts at the national level are collectively known as authoritative sources. Authoritative sources are documents such as acts, regulations, national cybersecurity policy (NCS) and international treaties. These sources should be the starting point

and should be consulted first during the development of national cybersecurity frameworks. They would prescribe mandatory requirements from a legal and regulatory perspective to be included in the framework. During a nation state's national cybersecurity function management journey, the following elements need to be identified for it to determine mandatory national cybersecurity functions.

- National and international authoritative sources specific and relevant to the nation-state.
- Mandatory prescripts and requirements for national cybersecurity functions expressed in the nation state's relevant authoritative sources.

Mandatory prescripts are found mainly in authoritative sources. A prescript is a rule, directive, command or law. From a cybersecurity function perspective, and at the national level, a prescript will express mandatory requirements that have to be included, or considered during the identification of national cybersecurity functions.

Some examples of South African authoritative sources are the NCPF [33], the South African Cybercrimes and Cybersecurity Bill [34] and the Regulation of Interception of Communications and Provision of Communication-Related Information Act, 2002 (Act 70 of 2002) [35]. Identifying all these sources and following their prescripts ensure that the mandatory national cybersecurity functions, specific to the nation-state are identified.

One of the core tenets of the first level of our NCMF is that it first identifies, and then consults nation state specific, national and international authoritative sources that prescribe mandatory cybersecurity function requirements. We will now show in Section 2.6.2 that it is also possible to use an NCMF to identify general cybersecurity functions that are non-mandatory in nature.



### 2.6.2 General cybersecurity functions

The identification of general (non-mandatory) cybersecurity functions is done by considering only the general recommendations in national and international normative sources. Nations may also select to use the authoritative sources from other countries, and apply those as their normative sources.

The following needs to be considered during the identification of non-mandatory cybersecurity functions. These functions are, by definition, general in nature.

- National and international normative sources need to be identified.
- General recommendations for cybersecurity functions need to be identified.

## 2.7 General discussion of cybersecurity functions

Other than a country's legal and regulatory framework, an NCS is of paramount importance as an authoritative source to steer cybersecurity activities at national level. A well thought through NCS will have considered national and international acts and regulations, and have their prescripts and recommendations captured.

Therefore, the national cybersecurity prescripts found in a nation-state's NCS serve as our primary source to assist with the identification of *mandatory* national cybersecurity functions. With the application of the NCMF, the NCS is seen as a document of the highest authority, and the primary source of information on how cybersecurity matters at the national level should be conducted.

National and international authoritative source documents and their prescripts differ between countries, and this implies that mandatory national cybersecurity functions will differ from country to country. As an example, the national cybersecurity functions needed to support the Saudi Arabian National Cybersecurity Strategy "*Developing National Information Security Strategy for the Kingdom of Saudi Arabia"* [36] will differ from the national cybersecurity functions needed by South Africa, as prescribed in their "*National Cybersecurity Policy Framework*" [33].

The Kingdom of Saudi Arabia restricts social media, and in some instances, social media platforms are blocked in the country as prescribed by their NCS [37]. This differs from South Africa's open and tolerant stance on social media. The Saudi Arabian restrictive social media policy necessitates the requirement for an additional national cybersecurity function, which is one of being able to monitor, and block social media platforms at the national level.



Another additional national cybersecurity function requirement is a cyberwarfare function. Saudi Arabia is actively engaged in a cyberwar with Iran and Yemen [38], and a cyberwar function is thus a requirement.

South Africa is not at war, or engaged in cyberwar with other nations, and has no requirement for a cyberwarfare function. These two national cybersecurity functions are not currently a requirement in South Africa.

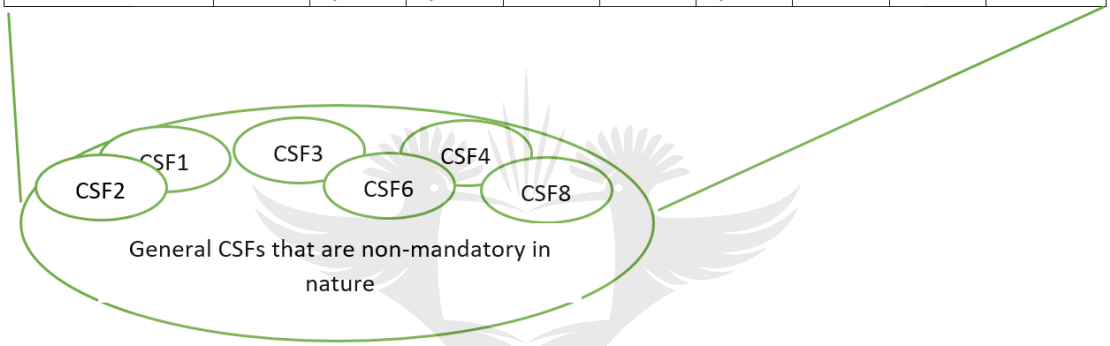
There might, however, be exclusions, in that mandatory national cybersecurity functional prescripts and requirements could be similar between nation states. Such an example is the South Africa Protection of Personal Information (POPI) Act [39], which is based on the United Kingdom's Data Protection Act of 1998 [40]. In this example, there may be similarities between the United Kingdom's

and South African national cybersecurity function prescripts and requirements needed to give effect to these two similar acts.

Table 1 shows that we may use national and international authoritative and normative sources to identify mandatory and non-mandatory cybersecurity functions. From these functions, we can identify the most commonly occurring functions to provide us with a list of general cybersecurity functions. We will do this in Chapter 4.

**Table 1: General CSFs from mandatory and non-mandatory CSFs**

| | CSF1 | CSF2 | CSF3 | CSF4 | CSF5 | CSF6 | CSF7 | CSF8 | CSF….$^{n}$ |
|---|---|---|---|---|---|---|---|---|---|
| **Mandatory CSFs** | ✓ | | | ✓ | | | | ✓ | |
| **General CSFs** | | ✓ | ✓ | | | ✓ | | | |




## 2.8 Other elements influencing the NCMF

Other elements such as the actors and stakeholders that are present and interacting with the NCMF, its dimensions, as well as the mandates and domains where the NCMF operates in, influences the identification, selection and prioritisation of national cybersecurity functions. These elements are discussed in detail in Chapter 3. The dimensions, mandates and domains also reside at the first level of the NCMF, and together with authoritative and normative sources, influence the consecutive levels of the NCMF. As a brief introduction, and to contextualise the dimensions, domains and mandates, they influence the following tasks:

- Dimensions describe the scope of something [41], such as the scope of national cybersecurity. Dimensions can be used to identify national and international actors and stakeholders (actors and stakeholders are introduced and discussed in Section 3.5). The availability of actors and stakeholders, and their skills, skills level and experience, in turn, influences the selection and prioritisation tasks.

- Cybersecurity activities can take place in the offensive, or defensive domains. Domains influence the selection and prioritisation task, in that different functions are needed to satisfy the offensive, or defensive domains' requirements.

- Mandates influence the selection and prioritisation task. The mandate describes the nation's authority to act in a certain way where it concerns national cybersecurity, and this, in turn, influences the functions selected and prioritised to satisfy the national cybersecurity mandate.

In conclusion, a country's national and international authoritative sources thus prescribe *mandatory* national cybersecurity functions, and it is our experience that developing countries often lack national authoritative sources, such as an NCS. In instances where nation states lack national authoritative sources, they may wish to identify *non-mandatory* cybersecurity functions by consulting recommendations in national and international normative sources.

They may further choose to augment their normative sources with mandatory prescripts found in other nations' authoritative sources. In other words, they may use other nation's mandatory functions as their non-mandatory functions. This approach provides nation states with a list of general cybersecurity functions. From this list of general functions, they may then select one or two functions for implementation at the national level.

The selection and prioritisation of cybersecurity functions for national implementation, are also influenced by the cybersecurity dimensions, domains and mandates. We will discuss this in Chapter 3. The authoritative source prescripts, the normative source recommendations, as well as the influencing dimensions, domains and mandates all reside at the first level of the NCMF.



## 2.9 A high-level overview of the NCMF levels

The identification of cybersecurity functions happens at the first level of the NCMF. This is done by consulting national and international authoritative and normative sources. The selection and prioritisation of national cybersecurity functions for implementation are described, and achieved at the second level of the NCMF. This is achieved by following a national risk management approach.

The selection and prioritisation of national cybersecurity functions for implementation may be further guided by the NCMF domains and mandates. The implementation of national cybersecurity functions and their structures is described in levels 3 to 6 of the NCMF. This concept is shown in Figure 11.

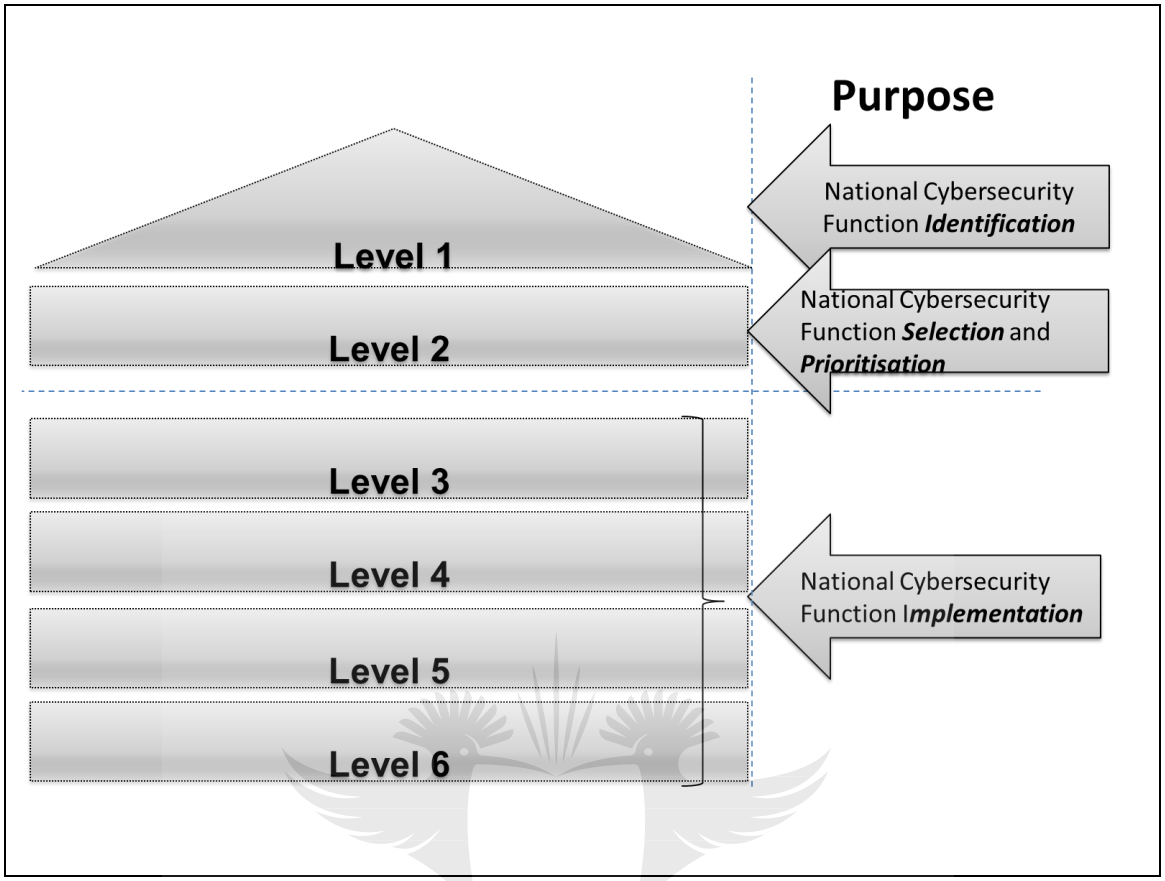



**Figure 11: NCMF purpose to level mapping**

During the identification of the NCMF levels, we drew from our experience in developing cybersecurity frameworks and architectures for the South African Government, as well as for the industry. Our experience includes a national collaborative project that was executed in terms of the national cybersecurity capability deployment strategy for South Africa [42].

As stated in Section 1.3, some of the characteristics of the NCMF is that it should be able to scale at the national level, and it should be flexible, and agile. With regard to satisfying these requirements, we have made a conscious decision to keep the NCMF lean and compact. Furthermore, it is our experience that a framework with more than ten levels becomes complicated, and it makes the implementation and execution thereof difficult. Experience has shown that frameworks with ten or fewer levels are easier to implement, monitor and manage.

Thus, we initially decided to constrain the development of the NCMF to ten levels, but less than ten are preferable to make it less complex, and to streamline its implementation. After having considered all the elements needed to provide an input into the NCMF to identify, select, prioritise, and implement national cybersecurity functions, we ended up with the six levels.

Our NCMF thus consists of six sequential levels, starting at level 1 and ending at level 6. Figure 11 shows that level 1 has as its purpose, the identification of cybersecurity functions, and that the purpose of level 2 is to select and prioritise the functions for implementation. Levels 3 to 6 describe the implementation of cybersecurity functions. Our NCMF's six levels that will be discussed in detail in the following Chapters. We will provide a brief introduction to the NCMF's six levels in the sub-sections following.

### 2.9.1 First level – Level 1 (L1)

The purpose of the first level, named **level 1**, is to ***identify national cybersecurity functions***. This is done by identifying national and international authoritative and normative sources, and the cybersecurity function prescripts and recommendations expressed in them. The authoritative source prescripts identify mandatory national cybersecurity functions, while the normative source recommendations describe non-mandatory cybersecurity functions. Additional elements, influencing the cybersecurity management tasks, as well as their impact on cybersecurity functions, are also considered here.

The additional influencing elements are the dimensions, mandates and domains in which the framework will operate. These additional influencing elements are discussed in detail in Chapter 3. The outcome of level 1 of the NCMF is a list of mandatory and non-mandatory national cybersecurity functions, from which a selection may be made for national implementation. Level 1 also identifies and lists NCMF actors. The identification of NCMF actors is discussed in Chapter 3.

From the list of NCMF actors, some can be selected to be held responsible for the application and implementation of the NCMF. Responsibility for the national implementation of the cybersecurity functions may also be assigned to the actors identified and presented in the list — the mandates and domains selected at level 1 further influences the selection and prioritisation of national cybersecurity functions for implementation.

Level 1 is foundational in nature, in that is must be completed first, before any of the other NCMF levels can be completed. It will not be possible to progress with levels 2 to 6 unless level 1 is completed, since the rest of the framework depends on the outcomes of level 1. The outcomes of level 1 feed into the rest of the NCMF levels.

Due to its foundational nature, level 1 of the NCMF is discussed in detail on its own in Chapter 3. The next step is to do the actual selection and prioritisation of national cybersecurity functions for implementation. This step is described in level 2 of the NCMF.

### 2.9.2 Second level – Level 2 (L2)

The purpose of the second level of the NCMF, named **level 2**, is to ***select and prioritise*** national cybersecurity functions for implementation. To ensure implementation of the NCMF, and to execute the selection and prioritisation of national cybersecurity functions for implementation, an overall controlling and coordinating body must be established. The selection and prioritisation of cybersecurity functions for national implementation may be facilitated by following a national risk management approach. The second level describes the establishment of:

- A national, overall cybersecurity controlling and coordinating body, with the purpose of implementing the NCMF, and to drive the selection and prioritisation of cybersecurity functions for national implementation, as well as,
- A national risk management approach to guide the selection and prioritisation of cybersecurity functions for national implementation.

The purpose of the national overall controlling body would be to manage, drive and apply the NCMF, and to steer, coordinate and assign responsibilities for the implementation of national cybersecurity functions. The establishment of the overall controlling body is key to the success of not only implementing and driving the NCMF and its efforts, but also the national implementation of the cybersecurity functions. The overall controlling body will only be successful with the implementation of the NCMF and the cybersecurity functions if appointed by government, allocated adequate funding and resources, and provided with a clear mandate. The national overall controlling body will also oversee the implementation of a national risk management approach and process.



From experience, we propose that a risk management approach and process is followed to help with the selection and prioritisation of cybersecurity functions at the national level. Following a risk management approach where it concerns the management of national or organisational cybersecurity risk, is also recommended by international standards such as the International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC) 27001:2013.

The outcome of the national risk management process may ***inform the selection*** of cybersecurity functions, and will primarily ***prioritise*** national cybersecurity functions for implementation. The NCMF mandates and domains may also influence the selection and prioritisation of national cybersecurity functions, while the NCMF dimensions are used to identify NCMF actors and stakeholders. The outcome of level 2 of the NCMF is a list of selected and prioritised national cybersecurity functions to be considered for implementation. **Level 2's** primary function is to ***prioritise*** national cybersecurity functions for implementation. This is achieved by developing a

national cybersecurity risk management strategy that describes a risk management framework and process. This strategy and process are driven by the overall cybersecurity controlling body.

### 2.9.3 Third level – Level 3 (L3)

The third level of the NCMF, named **level 3**, serves to consolidate the national cybersecurity functions selected and prioritised in level 2. The intention is for this level to be used to group a nation's national cybersecurity functions logically. The existing cybersecurity structures offering the cybersecurity functions are also identified here. In the absence of existing structures, new structures should be envisioned and implemented.

Level 3 is also the demarcation point in the NCMF where the ***implementation*** of national cybersecurity functions starts. In our NCMF, the implementation of national cybersecurity functions will be guided by the Build, Run and Monitor functions of the PBMR organisational approach.

### 2.9.4 Fourth level – Level 4 (L4)

**Level 4,** the fourth level of the NCMF, identifies and provides a placeholder to consolidate the national cybersecurity structures that will be used to offer the national cybersecurity functions (from level 3) and its services. The national cybersecurity structures are identified using the cybersecurity functions found in level 3, as input. The outcome of level 4 is a list of national cybersecurity structures, and the services they need to offer to enable the national cybersecurity functions. This list could be used by developing countries to identify overlapping and similar services and to combine their processes and technologies to realise a cost and skills saving.



### 2.9.5 Fifth level – Level 5 (L5)

The fifth level, named **level 5**, of the NCMF is used to identify the prescripts expressed in regulations and normative sources that are applicable to the cybersecurity structures that were identified in level 4. The outcome of level 5 is a list of prescripts that the cybersecurity structures from level 4 need to comply with. These prescripts will influence the level 4 structures' operational and technical requirements.

Where this is a new structure, these regulations and normative sources may need to be developed. Level 5 of the NCMF determines the level 4 cybersecurity structures' applicable authoritative and normative source prescripts. The level 4 structures need to comply with these, and other regulatory requirements identified in level 5. One authoritative source example applicable to South African organisations, is the Occupational Health and Safety Act (No. 85 of 1993) [43].

### 2.9.6 Sixth level – Level 6 (L6)

The sixth level, named **level 6**, is used to identify operational policies, processes and procedures to govern and manage the national cybersecurity structure. Level 6 addresses the operational elements of the national cybersecurity structure, and the outcome of level 6 is the cybersecurity structure's operational policies, processes and procedures.

## 2.10 Difference between level 5 and level 6 prescripts

The reader needs to have a clear understanding of the difference between the authoritative and normative source prescripts needed at level 5 (Section 5.3.4), and level 6 (Section 5.3.5). We will now describe this distinction in more detail.

- **Level 5 prescripts**: The national cybersecurity structures are identified in level 3, and their services in level 4. The prescripts that are relevant to national structures structure are identified in level 5. These are prescripts found in national or international authoritative and normative sources and are strategic in nature.

  To contextualise this, we will use as an example a nation that wants to establish a CSIRT to offer the Incident Handling function. Since this is a national structure, prescripts from the following international and national authoritative sources may apply:

  - To join the Forum of Incident Response and Security Teams (FIRST) [44] community, the national CSIRT has to comply with their mandatory requirements [45].
  - Being a national, government structure, the CSIRT has to comply with the nations' environmental health and safety acts, and possible national physical security regulations if the CSIRT is seen as a critical national asset.
  - The CSIRT, falling under the auspices of government would need to comply with departmental recommendations, such as the use of COBIT 5.

- **Level 6 prescripts:** The prescripts and recommendations that need to be developed, at level 6 are operational in nature. These operational sources are typically the policies, processes and procedures that govern the day to day operations of the national structure.

  Whereas the prescripts at level 5 may be applicable to all government structures, the prescripts at level 6 are structure specific. These source prescripts are usually developed by the structure management. Keeping with the CSIRT example, the following may need to be developed:

- Incident classification policy.
- Incident management and escalation process.
- Backup-up process and technology specific back-up procedure.

## 2.11 NCMF levels and level purpose

The NCMF levels and their explicit purpose are listed in Table 2. Table 2 shows that the primary function of level 1 of the NCMF is to identify national and international authoritative and normative sources and consult those sources to ***identify mandatory, and non-mandatory cybersecurity functions***.

Level 2 is used to ***select and prioritise the identified national cybersecurity functions for implementation.*** Level 3 is used as a container to consolidate the national cybersecurity functions logically.. Level 3 also serves as the demarcation point where the ***implementation of national cybersecurity functions*** starts.

Level 1 and level 2 correspond to the plan function of the PBMR organisational approach, while level 3 to level 6 correspond to the Build, Run and Monitor functions of the PBMR organisational approach. Level 4 identifies existing structures that can offer the selected and prioritised functions or envision new structures where none exists.

Level 4 also identifies the functions offered by existing structures or identify functions for new structures. Level 5 identifies the services that support the level 4 structure's functions, as well as authoritative and normative source prescripts applicable to the level structures. Level 6 describes the operational elements such as policies, processes and procedures needed to make the level 4 structure work.

These levels may be used to implement any cybersecurity structure, but in this thesis, we will use it to implement our newly envisioned national cybersecurity structure. The concept that levels 3 to 6 may be used for any national cybersecurity structure is explained in more detail in Section 5.2.

**Table 2: NCMF level explicit purpose**

| NCMF Level | Explicit Purpose |
|---|---|
| **National cybersecurity identification function** | |
| **NCMF Level 1 (L1)** | • This is the NCMF foundational level.<br>• This level identifies national and international authoritative and normative sources, with their mandatory and non-mandatory cybersecurity function prescripts and recommendations. |

| | |
|---|---|
| | • The mandates and domains that are considered at level 1 assist to identify national cybersecurity functions.<br>• The dimensions identify actors. Level 1 is used to identify national cybersecurity functions and provide a list of actors responsible for the NCMF, and for the implementation of the cybersecurity functions. |
| **National cybersecurity selection and prioritisation function** | |
| **NCMF Level 2 (L2)** | • Prescribes an overall national controlling body that will implement, guide and steer the NCMF application, as well as the national cybersecurity function implementation.<br>• Also prescribes a national cybersecurity risk management approach with the purpose of selecting and prioritising national cybersecurity functions.<br>• Selection and prioritisation of national cybersecurity functions for implementation happen here. |
| **National cybersecurity function implementation** | |
| **NCMF Level 3 (L3)** | • Serves as a placeholder to logically group and consolidate the selected and prioritised national cybersecurity functions. |
| **NCMF Level 4 (L4)** | • Identifies the existing national cybersecurity structure that will be used to offer the services of the cybersecurity functions identified in Level 3.<br>• Where no existing structures exist, new structures need to be envisioned and implemented. |
| **NCMF Level 5 (L5)** | • Identifies the services offered by these structures.<br>• Identifies authoritative and normative documents, and the national prescripts applicable and specific to the national cybersecurity structures identified in level 4. |
| **NCMF Level 6 (L6)** | • Describes the governance and operational management of the national cybersecurity structures.<br>• Identifies all structure specific, operational policies, processes and procedures. |

Table 2 also serve to provide the reader with a brief overview of Part 1 of this thesis. The levels introduced and briefly described in Table 2 are revisited and discussed in more detail in Chapter 3 and Chapter 5.

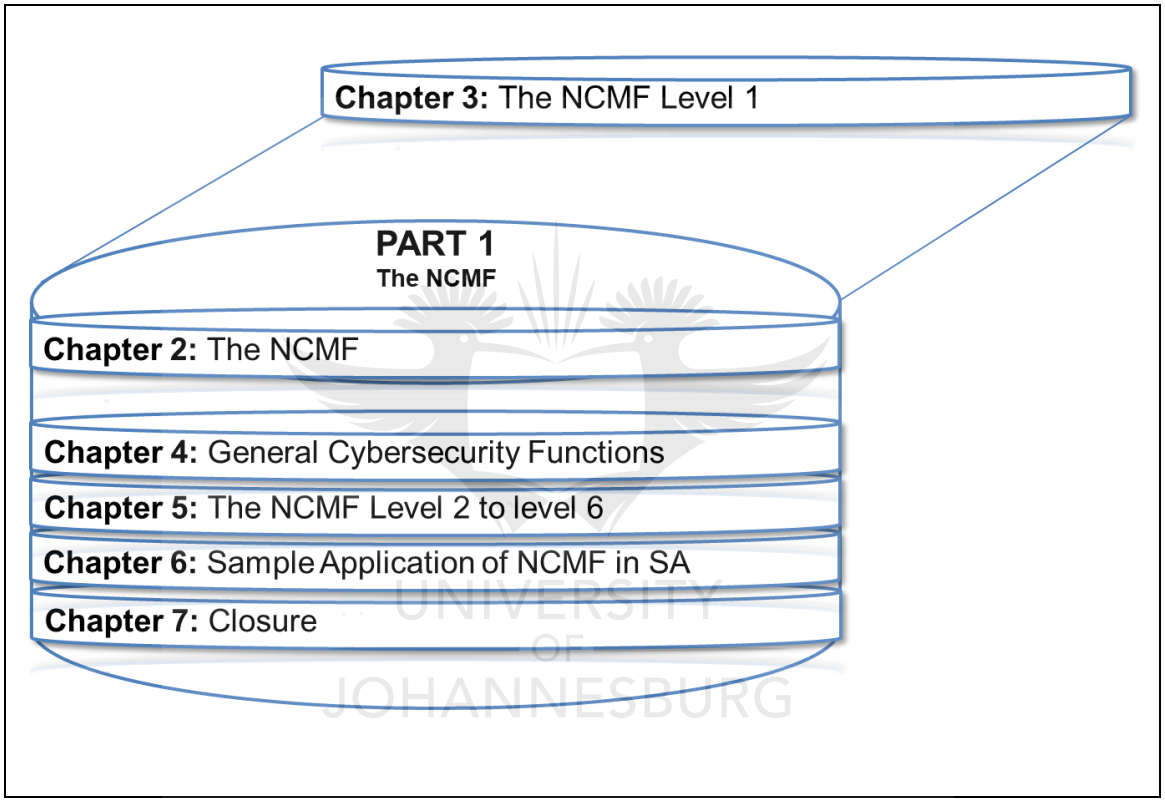
## 2.12 Conclusion

The prescripts for national cybersecurity functions are expressed in national authoritative and normative sources, and is used by the NCMF's first level for the ***identification*** of the mandatory cybersecurity functions. The recommendations found in national and international normative sources, allows the NCMF to identify non-mandatory cybersecurity functions.

The NCMF mandates and domains may influence and inform the identification, selection and prioritisation of national cybersecurity functions, while the NCMF dimensions are used to determine actors at level 1 of the NCMF. These influencing elements are introduced and discussed in Chapter 3.

The second level of the NCMF prescribes an overall national controlling body, and the following of a national cybersecurity risk management approach. The second level serves to ***select and prioritise*** national cybersecurity functions for implementation. The third to sixth levels of the NCMF prescribe a methodology to be followed for the implementation of national cybersecurity functions.

Taking into consideration the importance and foundational nature of level 1 of the NCMF, and the fact that the success and relevance of the identified, selected and prioritised national cybersecurity functions rely on accurate and applicable information from level 1, it will be discussed in a chapter on its own. Chapter 3 presents level 1 of the NCMF, with its building blocks and influencing elements



# Chapter 3: The national cybersecurity management framework level 1

## 3.1 Introduction

Chapter 3 introduces the elements that inform and influence the identification of mandatory national, and general cybersecurity functions. We have introduced elements such as national and international authoritative and normative sources, and their mandatory and general prescripts and recommendations in Section 2.6. Examples of other elements influencing the identification of cybersecurity functions are the dimensions and domains that the NCMF operate in, as well as its mandates. These influencing elements reside, and are considered at the first level of the NCMF - which is called level 1. These elements are discussed in the following sections.

These elements are applicable and specific to the nation applying the NCMF, and must be considered for guidance. The dimensions describe *who* is involved with national cybersecurity, such as the actors that can be found in each dimension. The domains describe where national cybersecurity activities take place. The mandates stipulate in what way a nation should act to ensure cybersecurity at the national level. The rest of Chapter 3 is structured as follows:

**Section 3.2** provides a motivation for the existence of level 1 of the NCMF, and its overall purpose in the NCMF.

**Section 3.3** introduces and discusses the concepts of national and international authoritative and normative sources.



**Section 3.4** motivates for the early discussion and identification of general cybersecurity functions.

**Section 3.5** introduces and discusses the three cybersecurity dimensions.

**Section 3.6** introduces two cybersecurity domains.

**Section 3.7** contextualises the Domains and Actors in the South African environment.

**Section 3.8** introduces five cybersecurity mandates.

**Section 3.9** contextualises the dimensions and mandates in the South African environment.

**Section 3.10** concludes and summarises level 1 of the NCMF, and the elements making up level 1. The elements are the authoritative and normative sources, dimensions, domains and mandates.

It needs to be mentioned here that Chapter 3 is quite a long chapter. We have made a conscious and intentional decision to keep all the level 1 elements under discussion, grouped in this chapter so that the flow of the level 1 elements under discussion is not disrupted.

## 3.2 Motivation

Level 1 of the NCMF serves as the starting point for the NCMF, and is the foundation on which the rest of the NCMF levels are developed. Level 1 of the NCMF provides input into, and drives the rest of the NCMF. The quality of the information provided by level 1 determines the relevance, accuracy and effectiveness of the identified, selected and prioritised national cybersecurity functions.

It further influences the successful application of the NCMF's subsequent levels, and how effective the NCMF will be in improving a nation's cybersecurity posture. In short, and to repeat what we have said in Section 2.5, level 1 is used to identify national and international authoritative and normative sources, and from those sources, identify prescripts for mandatory cybersecurity functions, or recommendations for non-mandatory cybersecurity functions. Level 1 also considers additional influencing elements such as dimensions, domains and mandates.



Providing accurate and relevant information at level 1 of the NCMF is of paramount importance. Inaccurate information at level 1 will cause level 2 to level 6 to be flawed, and thus irrelevant and ineffective in terms of the cybersecurity functions identified. The result could be that national cybersecurity functions that is not priority, or even irrelevant to the nation state's needs and requirements, are identified and selected for implementation. This could lead to national cyber risk not being addressed properly, and provide nation states with a false sense of security that may negatively affect their national cybersecurity posture and readiness.

Many elements can influence the quality of information at level 1. One of these is the authoritative and normative sources applicable to the nation-states. These authoritative and normative sources could be international or, national in origin. Some examples are:

- **International authoritative**
  - International law such as the Tallinn Manual is applying international law to cyberspace [46].

- Treaties and agreements, such as treaties and international agreements on Cyber Crime [47].

- **National authoritative**
  - National cybersecurity strategies.
  - A national policy such as the South African National Cybersecurity Policy Framework [6].
  - Acts such as the South African Cybercrimes and Cybersecurity Bill [34] and the Protection of Personal Information Act [39].
- **Normative**
  - Standards such as ISO/IEC 27001:2005 [48].
  - Frameworks such as COBIT [49], NIST SP 800-53 [50], and SANS Critical Security Controls [51].
  - Guides such as the ITU-T X.805 National Cybersecurity Strategy Guide [52].
  - Models such as the United Kingdom's Cyber Security Capability Maturity Model (CMM) [53].

From authoritative sources, prescripts for mandatory national cybersecurity functions are identified. From normative sources, recommendations for non-mandatory cybersecurity functions, are identified.

Once the mandatory and non-mandatory cybersecurity function requirements and recommendations expressed in these sources are identified, additional elements such as the dimensions, mandates and domains within which the NCMF will operate, need to be considered. These additional elements inform and influence the selection and prioritisation of both mandatory national cybersecurity functions, and non-mandatory cybersecurity functions.

The elements used to identify cybersecurity functions were introduced in Section 2.6. These are national and international authoritative and normative sources. Elements informing and influencing the selection and prioritisation of cybersecurity functions are the dimensions, mandates and domains. All these elements reside at level 1 of the NCMF.

To make it easier for the reader to understand and follow this chapter, our progress during the development of level 1 of the NCMF and its influencing elements is illustrated using Figure 12. Figure 12 shows the four elements making up level 1 of the NCMF, and each element will be highlighted during its discussion.

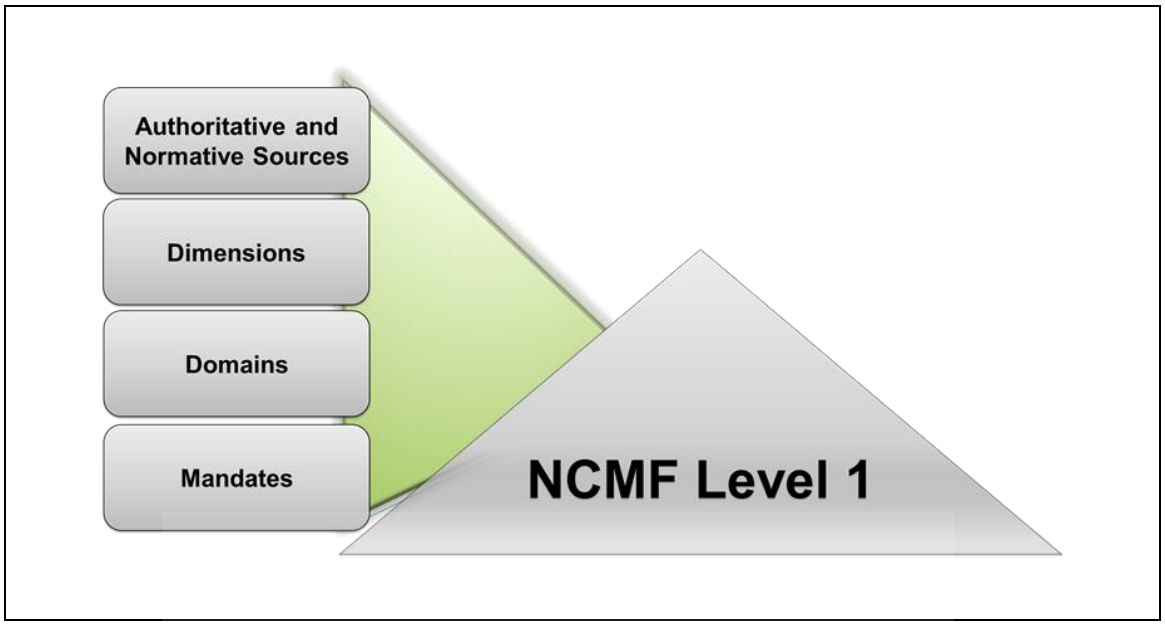



**Figure 12: Chapter 3 Section orientation**

Section 3.3 introduces the concept of 'authoritative and normative sources.' Under the authoritative sources, mandatory national cybersecurity prescripts are identified, and from the normative sources, general cybersecurity recommendations are identified. These sources could be national or international in origin.

## 3.3 NCMF Level 1 – Identify authoritative and normative sources

Figure 13 serves to orient the reader, and shows that this section will be used to discuss the NCMF authoritative and normative sources. Figure 13 shows that the authoritative and normative sources are the first element that makes up level 1 of the NCMF and that the authoritative and normative sources are used to identify mandatory and non-mandatory national cybersecurity functions.

Level 1 serves to identify authoritative and normative sources and its cybersecurity functional requirement prescripts and recommendations. These sources prescribe mandatory national functions or recommend non-mandatory cybersecurity functions. This level indicates the starting point of the NCMF, and serves as a flexible placeholder for input into the rest of the framework.

Level 1 is flexible in that authoritative and normative source prescripts and recommendations that are specific and unique to each nation-state, are identified and used here. Level 1 will be updated as and when a nation's authoritative and normative sources and their prescripts or recommendations change. The foundational character of this level is indicated by it's name,

"Level 1", and it has to be considered before any of the following levels of the framework can be used.

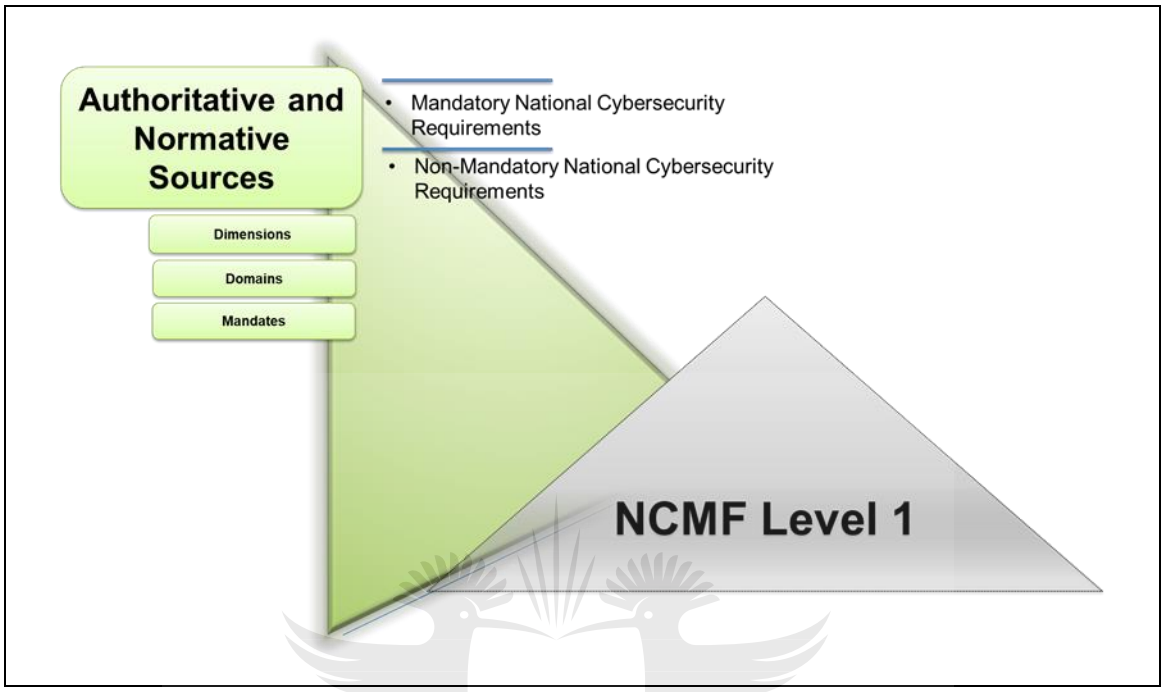



**Figure 13: Section 3.3 Orientation – Authoritative and normative sources**

An example of legal authoritative sources is shown in Figure 14 as taken from [54]. Figure 14 shows that a nation state's authoritative legal prescripts originate from rules, regulations and acts which then becomes law.

To illustrate the concept of a mandatory prescript, we will use the NCPF as an example of a South African authoritative source. A prescript found in the NCPF is that South Africa should have a national incident handling function [6]. Nation states must comply with authoritative sources. This is done to give effect to national policy prescripts, to avoid sanctions, to promote the national cybersecurity policy and strategy, and to comply with treaty obligations.

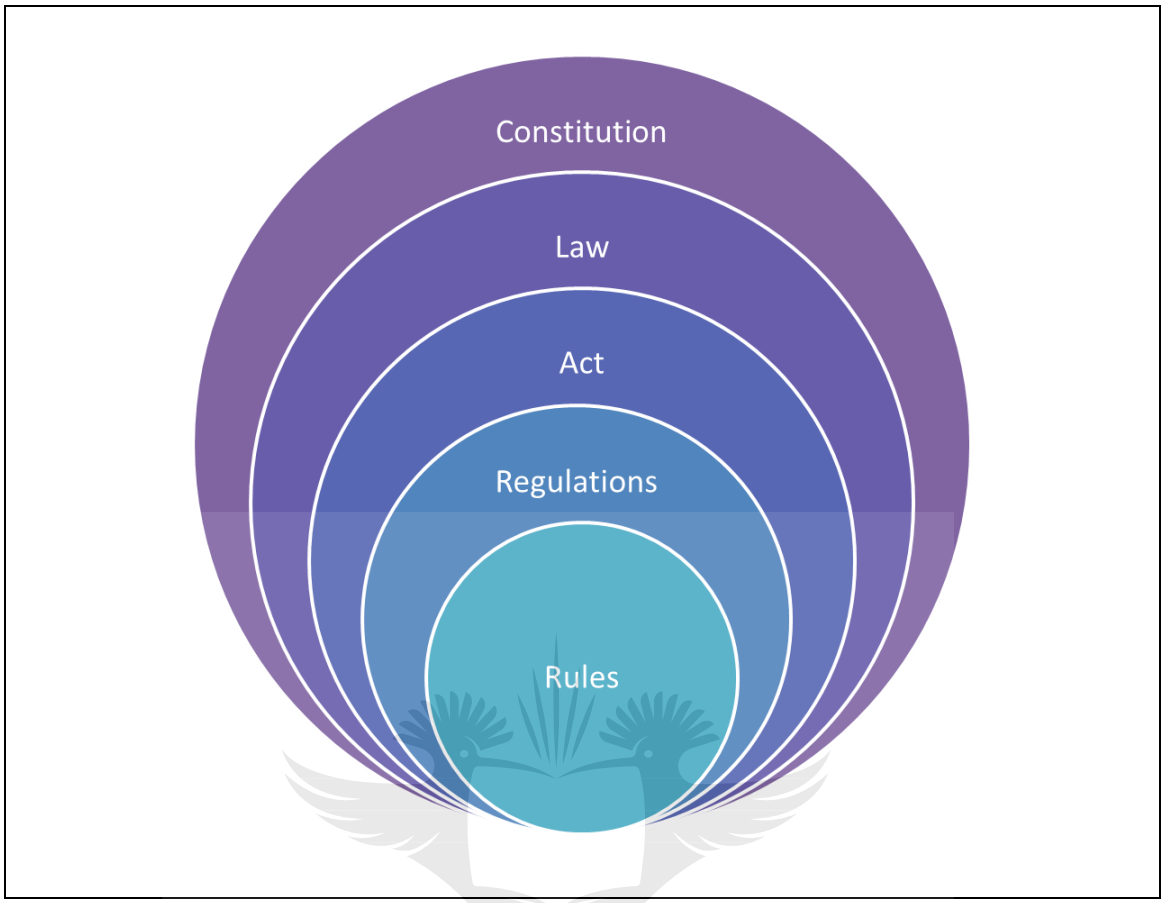



**Figure 14: Examples of authoritative sources** [54]



The responsibility for enforcing compliance to these laws, policies, strategies and treaties, resides with the government, and is achieved through the parliamentary processes applicable to the development of national policy, strategy and treaties. We will use level 1 of the NCMF to identify two types of cybersecurity functions. The two types are:

- Nation-state specific and mandatory cybersecurity functions.
- General or non-mandatory cybersecurity functions.

### 3.3.1 Identify mandatory national cybersecurity functions

To use level 1 of the NCMF to identify *nation state specific and mandatory cybersecurity functions*, we should start with:

- Identifying all national and international authoritative sources applicable and relevant to the natio- state.

- Identify mandatory, and nation-state specific, cybersecurity function prescripts expressed in these sources. The outcome is a list of mandatory national cybersecurity functions.

### 3.3.2 Identify non-mandatory cybersecurity functions

In the absence of national and international authoritative sources, nation-states may choose to identify non-mandatory cybersecurity function recommendations that can be found in national and international normative sources. This provides them with a list of cybersecurity functions from which they may select one, or two for implementation at the national level.

Another very good source that can be consulted to identify non-mandatory cybersecurity functions, are the NCSs of both developed and developing countries. Nations consulting the NCSs of foreign countries' in this way thus use the consulted foreign county's authoritative source as their normative source.

To use level 1 of the NCMF to identify *non-mandatory cybersecurity functions,* we should start with:

- Identifying national and international normative sources.
- Identify non-mandatory cybersecurity function recommendations. The outcome is a list of non-mandatory cybersecurity functions.

## 3.4 Motivation for early identification of general cybersecurity functions

We will illustrate the application of level 1 of the NCMF in Chapter 4 to identify general cybersecurity functions. We will do this by identifying prescripts in authoritative sources, and recommendations in non-mandatory sources. From these prescripts and recommendations, we will identify the most commonly occurring cybersecurity functions across international and national authoritative and normative sources to give us a list of general cybersecurity functions.

This predetermined list of general cybersecurity functions then provides us with a list of cybersecurity functions that is available to nation states to make a selection from for implementation. Our motivation for doing this early, and before the discussion of level 2 to level 6 of the NCMF is as follows:

- Our list of general cybersecurity functions are non-mandatory in nature, and will be used to illustrate and explain the application of the rest of the NCMF. From the list of general cybersecurity functions, we will select two functions to illustrate and explain level 2 to level 6

of the NCMF. This allows us to use real-life examples, and contextualise our discussion of levels 2 to 6.

- The process followed during the identification of mandatory and non-mandatory cybersecurity functions are the same, only the sources differ. The illustrative application of level 1 of the NCMF in Chapter 4 could thus be referenced for the identification of both mandatory and non-mandatory cybersecurity functions. Describing the identification process early informs and guides the discussion of the rest of the NCMF levels.
- Identifying general (which is by definition non-mandatory) cybersecurity functions provide nation-states that do not have their own authoritative sources, with a predetermined list of cybersecurity functions. They may then select and prioritise one or many functions from this list for implementation at the national level. This allows nation states that are applying the NCMF to make a selection of cybersecurity functions for implementation early on.

Now that the concepts of 'authoritative' and 'normative' sources have been introduced, other elements informing and influencing the selection and prioritisation of national cybersecurity functions need to be described and considered. These elements are the dimensions, mandates and domains in which the NCMF can operate. Section 3.5 introduces the national cybersecurity dimensions.

The cybersecurity dimensions in which the NCMF can operate, are the government dimension, the national dimension and the the international dimension. The dimensions have actors and stakeholders, and we will use the dimensions to identify the NCMF actors and stakeholders.

From the list of actors and stakeholders, responsibilities should be assigned for the establishment of the national, overall controlling body residing at level 2, and introduced in Section 5.4. The national, overall controlling body would be responsible for the implementation of the NCMF, and also the implementation of the cybersecurity functions identified through the application of the NCMF.

## 3.5 Cybersecurity dimensions actors and stakeholders

Figure 15 serves to orient the reader, and shows that this section will be used to discuss the NCMF Dimensions. The three Dimensions as taken from NATO, are:

- Government
- National
- International

A dimension describes the element or factor making up an entity, such as national cybersecurity, or describe the range or degree to which national cybersecurity stretches [55]. The cybersecurity dimensions are important since it will be used to identify nation state specific actors and stakeholders, and also inform the selection and prioritisation of national cybersecurity functions.

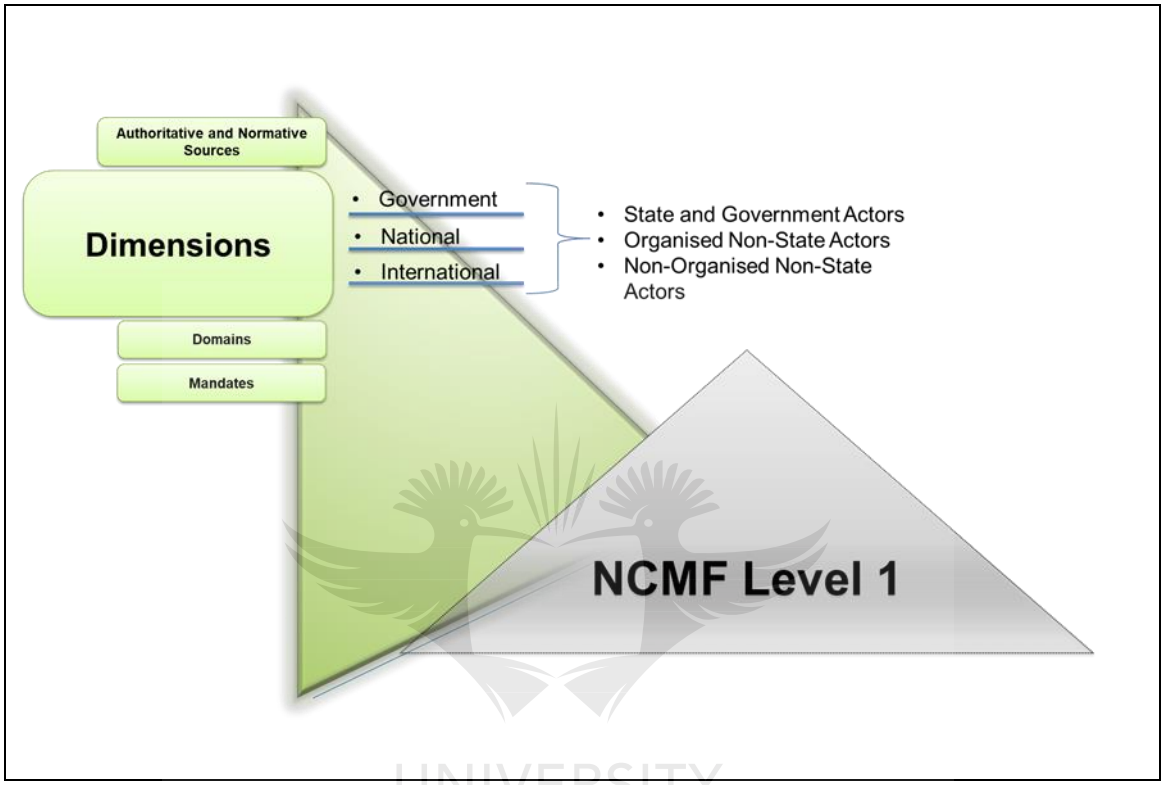





**Figure 15: Section 3.4 Orientation - dimensions**

The dimensions are the government dimension, the national dimension and the international dimension, and each dimension has state actors, non-state actors and non-state actors abroad. The identification of the actors allows nation states to assign responsibilities for the implementation of the NCMF, as well as responsibility for the implementation of national cybersecurity functions to them. Some of these actors may be selected to establish, and participate in the national overall controlling body.

The activities in these dimensions are influenced by stakeholders, and performed by actors. Each dimension has its own actors and stakeholders, and the government, national and international dimensions allow national cybersecurity to be viewed from the perspective of different actors and stakeholders such as political actors, and law enforcement or military stakeholders.

Before we introduce the three dimensions with its actors and stakeholders, it is important to understand the difference between them. The terms actor and stakeholder are often incorrectly used interchangeably, but they do differ. Actors can be either human or non-human, and are entities that perform activities, and interact with a project, system or product. An actor's behaviour is non-deterministic. Stakeholders are individuals or groups with an interest in a project, system or product. Stakeholder's behaviour is human, and they are deterministic. All stakeholders are actors, but not all actors are stakeholders.

Examples of stakeholders in the context of the NCMF are government departments, hacker groups and the public. They determine, influence or effect the outcome of the NCMF. All these mentioned stakeholders can also be acting on the NCMF, but additional actors for the NCMF could be the IT systems supporting the planning, building, running and monitoring of the NCMF implementation and also the cybersecurity function implementation [56] [57] [58] [59] [60].

The dimensions identify the actors and stakeholders, and in turn, the availability of actors and stakeholders, and their skills may influence the selection and prioritisation of cybersecurity functions. Nation states may want to prioritise the implementation of cybersecurity functions for which actors and stakeholders with experience and skills are readily available, or use this information to align their training and certification requirements. To assist with the identification of actors and stakeholders, we will propose an Actor and Stakeholder Identification Template in Section 3.5.4.



Together with the authoritative and normative prescripts and recommendations, the dimensions thus informs and influences the selection and prioritisation of cybersecurity functions for implementation. It also assists with the identification of actors and stakeholders. NATO, in their National Cybersecurity Framework Manual document [1], described three dimensions of cybersecurity activity. These three dimensions describe the actors and stakeholders across five different mandates (see Section 3.8). In turn, the five mandates can take place in two cyber domains- [1] (see Section 3.6). The three cybersecurity dimensions are:

- **Dimension 1**: Government dimension.
- **Dimension 2**: National dimension.
- **Dimension 3**: International dimension.

During the presentation of the NCMF levels, we will identify both stakeholders and actors, but the focus will be on actors only, since responsibility for the execution of the NCMF, and implementation of national cybersecurity functions are assigned to them. Furthermore, actors include systems (technology), as well as products. The NCMF actors are all the entities (human, IT and other

systems) interacting with the NCMF. The following actor types are found across all three dimensions and must be considered during the application of the NCMF. We now provide a description of the actor types, and illustrate that all three actor types are found across the dimensions in Table 3:

- **State and government actors** - these are inclusive of all state and government sector entities, as well as public sector entities existing within a country's borders [1].
- **Organised non-state actors** - these are groups such as hackers, cyber militia, (state-sponsored or individual), and cyber-crime organisations. Vendors, security and defence contractors supporting the cybersecurity endeavours of states are also included in this group [1].
- **Non-organised non-state actors** - this group typically consists of individuals launching crime campaigns and hacktivism activity.

Table 3 visualises all the actor types can be found across all three the dimensions:

**Table 3: Dimensions and actor types**

| Government Dimension | National Dimension | International Dimension |
|---|---|---|
| State and government actors | State and government actors | State and government actors |
| Organised non-state actors | Organised non-state actors | Organised non-state actors |
| Non-organised non-state actors | Non-organised non-state actors | Non-organised non-state actors |



At a national level, the state needs to foster relationships with cybersecurity vendors, service providers and contractors, as well as critical infrastructure providers. These are called non-state actors, but they may play a role in securing the national cybersecurity domain [1]. These actors will be mapped to the NATO cybersecurity dimensions in Section 3.5.1 to Section 3.5.3.

This mapping will be done in the context of South African actors. We do this in order to provide us with a template that can be used to identify actors interacting with national projects, systems or products, such as the NCMF, as well as the national cybersecurity functions identified through the application of the NCMF.

The NCMF operates across all three NATO dimensions, and being a national framework, actors are present in all three dimensions, and need to be considered. Section 3.5.1 to Section 3.5.3 introduces the dimensions in a South African context [1].

### 3.5.1 Dimension 1: Government

The government dimension is known as Whole of Government (WoG), and it aims to improve co-ordination between different state departments. In the context of using South Africa as the reference developing country, this dimension includes the three spheres of the South African government. The three spheres are national, provincial and local government. Each sphere has its own legislative, executive and administrative structures.

The legislatures are elected members, and their purpose is to oversee the activities of the executives and administrative departments. They also approve law and national policies. The executive is the cabinet, and their role is to synchronise the development of law and national policies.

They further supervise the implementation of the law and national policies by the government departments. The government departments execute the tasks of government. They are accountable to the executive. The South African government spheres and their structures are shown in Table 4 as taken from [61]:

**Table 4: South African government spheres and their machinery** [61]

| Sphere | Legislature | Executive | Administration |
|---|---|---|---|
| **National** | Parliament | President and cabinet | Directors general and departments |
| **Provincial** | Provincial legislative | Premier and executive council | Heads of department (HoD) and staff |
| **Local** | Council | Mayor and mayoral committee | Municipal manager, HoDs and staff |

We have mentioned earlier that national cybersecurity may be viewed from three dimensions, and that there are actors and stakeholders operating in the three dimensions. The concept that the dimensions consist of actors is shown in Table 5.

Keeping in mind that the actors were defined as being either human or non-human, and are entities that interact with a project, system or product (see Section 3.5), it might in some instances happen that the state and government actors, organised non-state actors and non-organised non-state actors may be the same across all three dimensions.

A good example of this is the Anonymous Hacking Group that may, or may not, interact with projects, systems or products across the actors in all three dimensions. Hacking groups and

hacktivists are, by definition, always non-organised non-state actors across all three dimensions. Some of the South African state and government actors, organised non-state actors and non-organised non-state actors in the government dimension are shown in Table 5.

We further show in Table 5 that the state and government actors which could possibly act on the South African cyber domain, are typically government departments interacting with cybersecurity projects, systems, or products. It also shows that organised non-state actors are typically civil society groupings such as universities and research councils, and that non-organised non-state actors are any actor that has no organised structures.

The location of these actors could be national, or international, and their interaction on cybersecurity with projects, systems or products cannot be denied or overlooked. Due to the interconnected nature of nations and governments, international actors may inadvertently interact with, and influence cybersecurity projects, systems or products across all three dimensions.

**Table 5: Example of possible South African Government actors**

| Actors | Possible South African Government Actors |
|---|---|
| State and government actors | • Justice, Crime Prevention and Security Cluster (JCPS),<br>• Department of Defence (DOD),<br>• South African Police Service(SAPS),<br>• State Security Agency (SSA),<br>• Department of and Postal and Telecommunications Services (DTPS)<br>• Department of Justice (DoJ),<br>• Electronic Communications Security - CSIRT (ECS-CSIRT),<br>• Cybersecurity Hub. |
| Organised non-state actors | • Information Security Group Africa (ISG Africa).<br>• South African Cyber Security Academic Alliance (SACSAA).<br>• Centre for Cyber Security at the University of Johannesburg (UJ).<br>• South African Centre for Information Security (CIS).<br>• Council for Scientific and Industrial Research (CSIR) cybersecurity centre of innovation for South Africa.<br>• IT security vendors, and ISPs.<br>• Mobile operators.<br>• IT service providers. |
| Non-organised non-state actors | • Anonymous hacking group.<br>• LulzSec hacking group. |

### 3.5.2 Dimension 2: National

The national dimension is also known as the Whole of Nation (WoN), and the emphasis is on civil society, academia, ICT and security specialists and critical infrastructures. The aim is to establish and improve co-operation in terms of national and international cybersecurity matters.

Table 6 shows that the national dimension considers state and government actors, organised non-state actors and non-organised non-state actors which may interact with cybersecurity projects, systems or products at national level. The type of actors will differ from nation to nation, and depend on a nation's political make-up and organisation. Using South Africa as a reference country, State and Government Actors are provincial and local government structures. This includes Heads of Departments (HoDs) and municipalities as we have shown in Table 4. The different possible national actors from a South African perspective are shown in Table 6.

**Table 6: Example of possible national actors**

| Actors | Possible South African National Actors |
|---|---|
| State and government actors | • Provincial and local government structures such as national disaster management centres (NDMCs) and their HoDs |
| Organised non-state actors | • Information security group africa (ISG Africa),<br>• South African Cyber Security Academic Alliance (SACSAA),<br>• Centre for Cyber Security at the University of Johannesburg (UJ), South African Centre for Information Security (CIS),<br>• Council for Scientific and Industrial Research (CSIR) cybersecurity. centre of innovation for South Africa. |
| Non-organised non-state actors | • Anonymous and LulzSec hacking groups. |



### 3.5.3 Dimension 3: International

The international dimension is also known as Whole of Systems (WoS). Actors operating in the international dimension are diplomats, international technical work groups and internet governance stakeholders. The aim is to establish and facilitate collaboration. The different possible international actors from a South African perspective are shown in Table 7.

Table 7 shows that international actors could be foreign nation-states, as well as their departments concerned with cybersecurity. Examples are the United States Federal Bureau of Investigation (FBI) cybercrime investigative capability [62] and the United States Department of Homeland Security [63].

**Table 7: Example of possible international actors**

| Actors | Possible International Actors |
|---|---|
| State and government actors | • The other Nation States, Foreign Departments of Defence, Foreign Security Agencies, such as the Federal Bureau of Investigation (FBI), United States Department of Homeland Security |
| Organised non-state actors | • Forum of Incident Response and Security Teams (FIRST),<br>• Vendors such as Microsoft and Cisco |
| Non-organised non-state actors | • Anonymous and LulzSec Hacking Groups |

### 3.5.4 Rationale and sample application of dimensions

The main purpose for the consideration of the dimensions is thus to provide a mechanism to assist with the identification of NCMF actors specific to the nation-state applying the NCMF. The identification of NCMF actors will result in a list of possible actors to be considered, and to be made responsible for the application of the NCMF.

Responsibility for the implementation of cybersecurity functions may also be assigned to the actors identified. In Table 8 we propose an actor and stakeholder identification template that can be used to assist with the identification of national actors and stakeholders.

The intention is for entities applying the NCMF to use this template to identify their specific actors and stakeholders across the three dimensions, for each national cybersecurity function. Each entity making use of the Actor and Stakeholder Identification Template will populate the template with their actors and stakeholders across the three dimensions that are applicable to a specific national cybersecurity function.

We show in Table 8 a sample application of our Actor and Stakeholder Identification Template for the National Incident Handling function. Table 8 is populated with the actors identified in Table 5, Table 6 and Table 7. In our example, the actors identified n Table 8 will be assigned the responsibility to plan, build, run monitor, and interact with the National Incident Handling function. In some instances, where no suitable actors and stakeholders can be identified by using our template, nations may consider creating new roles, and assign responsibilities to new actors.

**Table 8: Actor and stakeholder identification template for national incident handling function**

| | Dimension 1 Government | Dimension 2 National | Dimension 3 International |
|---|---|---|---|
| **State and Government Stakeholders and Actors** | SSA, DTPS | NDMC | FBI |
| **Organised Non-State Stakeholders and Actors** | Universities, | ISPs | FIRST |
| **Non-Organised Non-State Stakeholders and Actors** | Nation | Vendors | Consultants |

An example of a new role could be that of executive cyber leadership, with the responsibility to initiate and construct the national cybersecurity mission and vision, and to steer and guide the national cyber resources and operations. For guidance on roles and responsibilities in terms of ICT, the Skills Framework for the Information Age (SFIA) [64] or NIST's National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework described in NIST SP 800-181 [65] may be consulted.

The national, overall controlling body (residing at level 2 of the NCMF, and introduced in Section 5.4) will be established by actors that are identified by using our template. Also, some of these actors will be selected to serve on the national overall controlling body. The responsibility for the implementation of selected and prioritised national cybersecurity functions is also assigned to the actors that are identified using our template.



Now that the discussion on dimensions is concluded, we will introduce and discuss the cyber domains in Section 3.6. We will introduce two domains: the Offensive and Defensive domains, and their lifecycle phases.

## 3.6 Cybersecurity domains – offensive and defensive

Figure 16 serves to orient the reader, and shows that this section will be used to discuss the two NCMF Domains as mentioned in NATO. The two domains are the offensive and defensive domains. The defensive domain lifecycle phases of prevent, detect, respond and recover are displayed.

The defensive domain lifecycle phases allow us to identify actors, functions and structures, and influences the selection and prioritisation of cybersecurity functions for implementation. As our intention is to illustrate the application of the NCMF in context of the defensive domain, we have only included the defensive domain lifecycle phases in Figure 16.

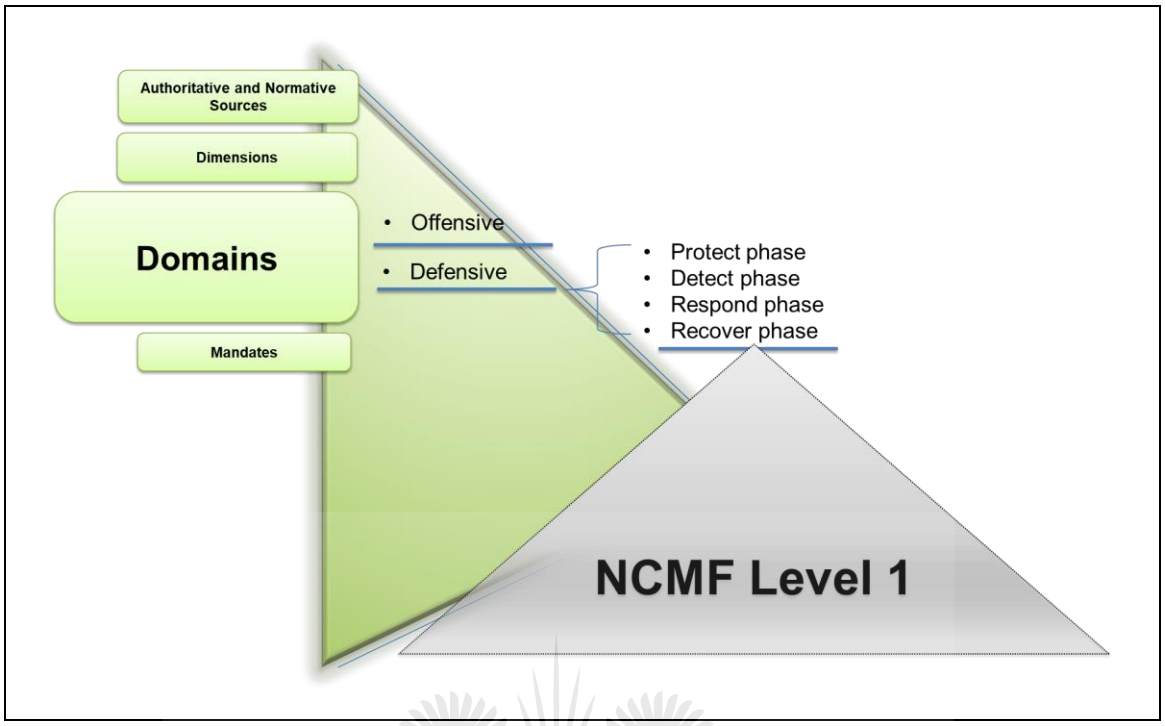



**Figure 16: Section 3.5 Orientation - Domains**

NATO identifies two domains in which cyber actions can take place. These are the offensive domain and the defensive domain. The lifecycle phases of the domains assist with the identification of cybersecurity structures from where cybersecurity functions are offered.. The offensive domain describe offensive actions in cyber, and the defensive domain describes defensive actions in cyber [1].

The offensive domain is typically the responsibility of a nation state's army, or intelligence agency. Cyber defence is the action of defending organisational or national ICT assets against attacks, discovering attacks, and to respond to, and recover from attacks and cybersecurity incidents. Both the offensive and defensive domains consist of lifecycle phases (see Section 3.6.1 and Section 3.6.2). The lifecycle phases serve to group the cybersecurity activities found in the domains logically, and this, in turn, provides input into the selection, and prioritisation of national cybersecurity functions.

The discussion of the lifecycle phases is important since they could influence the selection and prioritisation of both mandatory and non-mandatory cybersecurity functions. More importantly, the lifecycle phases could assist us with the identification of the cybersecurity structures needed to offer the national cybersecurity functions. Our rationale for introducing and discussing the cybersecurity domains is:

- **Rationale 1:** The cybersecurity domain in which the NCMF operate, will inform and influence the selection and prioritisation of mandatory national, and general cybersecurity functions. This is because the national cybersecurity functions needed, and its urgency for implementation will differ depending on whether the NCMF is applied in the context of the offensive or defensive domains.

  As an example, in the offensive domain, the focus could shift to national cybersecurity functions such as the establishment of a military cyber function, consisting of cyber warfare services, whereas in the defensive domain the focus could be on functions such as a national incident Handling function that consists of incident response services. In times of war, cybersecurity functions in the offensive domain will receive priority implementation over functions in the defensive domain.

- **Rationale 2:** The exploration of the activities taking place in the cybersecurity domain lifecycle phases assist with the identification of cybersecurity structures needed to offer national cybersecurity functions from. Different cybersecurity functions are needed during the different lifecycle phases, and these functions may be offered from different cybersecurity structures. Furthermore, as a complementary function to the dimensions, selecting an NCMF cybersecurity domain assists with the identification of actors.

Different actors are associated when comparing the offensive and defensive domains with each other, and this is illustrated in Table 10. To illustrate this in context of South Africa, the government actors in the offensive domain could be the South African Department of Defence (DOD), while government actors in the defensive domain could be the South African Department of Telecommunications and Postal Services (DTPS). Actors were introduced and discussed in Section 3.5.

Our intention is to illustrate the application of the NCMF in context of the Defensive domain since we have experience working in this domain. The purpose for the selection of a domain in which the NCMF operate, is thus to:

- Provide input into the selection and prioritisation of cybersecurity functions.
- Complement the identification of actors identified by the dimensions.
- Use the domain's lifecycle phases to assist with the identification of relevant national cybersecurity structures and its services, from where national cybersecurity functions, relevant to the domain lifecycle phases, will be offered from.

In Section 3.6.1. we will Introduce the offensive domain and its lifecycle phases briefly, and in Section 3.6.2, we introduce the defensive domain lifecycle phases. Analysis of the defensive domain lifecycle phases has two purposes.

**Purpose 1:** The first purpose is to assist us with the identification of existing cybersecurity associated functions and services. Identification of the cybersecurity structures allows us to identify, and to analyse the structure's functions and services. This, in turn, allows us to identify overlapping services and technologies which then could potentially be combined to realise a saving in terms of cost, and skills.

**Purpose 2:** The second purpose is to identify gaps in the existing structures. Each lifecycle phase's cybersecurity services may be offered from a different cybersecurity structure. Identifying the cybersecurity structures is important since this allows a nation-state to identify existing structures which could be used to offer national cybersecurity functions from. Where the ideal structure does not exist, or where there are gaps in the existing structures, the outcome of the analysis can form the basis for a gap analysis to drive the development and establishment of new national cybersecurity structures.

Section 3.6.1 briefly introduces and discusses the offensive domain.

### 3.6.1 Offensive domain

The purpose of offensive actions in cyber is to disrupt, destroy, steal and deny access to an adversary's systems. The NCSs of more than 30 countries describe dedicated offensive warfare programmes [1]. A well written NCS will describe the roles and responsibilities of actors in both the offensive and defensive domains.

Offensive actions are often framed as "attack". The offensive goals and actions differ between actors. As an example, non-state actors will launch cyber-attacks in order to steal information that can be sold (that is, credit card information), or to improve their status within their group. The actions of state actors may include spying, or theft of military or industrial secrets.

During armed conflict, state actors may also use cyber weapons in support of kinetic weapons, or in some cases to replace kinetic weapons. The offensive domain lifecycle phases are reconnaissance, initial compromise, command and control, lateral movement, target attainment, exfiltration, corruption, and disruption [66][67].

We will now be spending all our focus on the Defensive domain, since this is our domain of experience. The Offensive domain will not be discussed in further detail, and our illustrations and examples will be in context of the Defensive domain. Section 3.6.2 introduces and discusses the Defensive domain's four lifecycle phases, and identifies some of the existing structures from where the lifecycle phases' functions services may be offered from.

### 3.6.2 Defensive domain

Defensive actions in cyber has as purpose to protect organisations and nations' cyberspace against attacks. Activity in the defensive domain typically happens within the organisation, or nations networks [68]. The NATO proposes four cyber defence lifecycle phases. The four lifecycle phases proposed by NATO [1] are echoed by the United States Nuclear Regulatory Commission [69], NIST [70], and the United States National Security Agency (NSA) [71]. Furthermore, it corresponds to the NIST incident handling lifecycle phases [72] [73] [74]. The four lifecycle phases proposed by NATO, and others, are [1] [72] [73] [74]:

- Protecting phase.
- Detection phase.
- Responding phase.
- Recovering phase.

The discussion of the defensive domain's lifecycle phases is valuable in terms of identifying national, organisational, or commercial cybersecurity structures, and the cybersecurity services they offer during each of its lifecycle phases. Different structures offer different cybersecurity services across the different defensive domain lifecycle phases. It is our experience that commercial organisations often use a single structure to offer all the cyber defence life cycle phases.

As an example, a SOC can offer cybersecurity services to protect, detect, respond and recover from cybersecurity attacks and incidents at organisational level. However, at national level, different structures are often used to facilitate each of the individual defensive lifecycle phases such as using a national CSIRT to facilitate only the respond phase of the cyber defence lifecycle phase. The four defensive domain lifecycle phases, with their cybersecurity structures, are now introduced.

#### Phase 1: Protect

Phase 1 refers to the protection of national assets. A taxonomy may be used to categorise the security controls needed to protect national infrastructure. An example of such a taxonomy is

technical controls, administrative controls, and physical controls [75]. Technical controls describe controls that are technical in nature. Examples of technical controls are access control enforcers (firewalls) and end-point protection, such as anti-malware, while administrative controls are controls such as policies, processes, procedures, standards, best practices and guidelines.

Physical controls describe controls that are needed to enforce physical security. Examples are biometric access controls, guards and gates. Administrative controls are supported, and where possible, enforced by technical and physical controls. These protective actions are sometimes referred to as information assurance which describes the act of protecting all information, irrespective of which media it resides on [76].

It is important to establish a relationship between technical controls and the processes that they support to allow alignment with business, and the effective use of resources [77]. This is where disciplines such as Enterprise Information Security Architecture (EISA) comes into play [78] [79]. The cybersecurity operational services during the protect phase are commonly offered from a SOC structure at organisational level, and a Computer Emergency Response Team (CERT) or CSIRT[7] at national level.

## Phase 2: Detect

Phase 2 presumes that something has already happened. It is impossible to detect attacks before they have occurred, but attacks may be predicted. At a national level, intelligence and counter intelligence (CI) can assist with the prediction of attacks before they happen, and also detect attacks in progress, but when considering critical information infrastructure protection (CIIP), it is difficult to predict attacks before they happen.

This is because Intelligence and CI activities typically have a military application [1], and are used at national level to detect cyber attacks against nation states. Intelligence and CI activities are rarely part of the organisational cybersecurity effort. Experience has shown that organisations typically use cyber threat intelligence as a mechanism to predict attacks against the organisational assets.

Technical controls such as intrusion prevention systems (IPS), and intrusion detection systems (IDSs) typically provide a preventative function in that they use signatures to block attacks. They may also provide a detective function in that their logs can be analysed to detect attacks. This is an example of a technical control providing functions across the preventative and detective lifecycle.

[7] The terms CERT and CSIRT refers to the same structure.

The monitoring of these types of control logs typically happens in a SOC, and may be done by using Security Incident and Event Monitoring (SIEM) tools. SIEM tools can also be used to monitor ICT assets during all lifecycle phases. Another example of a technical control providing a detective function is automated vulnerability scanners, or penetration testing. The organisational ICT infrastructure should also be scanned pro-actively with vulnerability management tools to discover vulnerabilities that must then be mitigated.

Another detective control is file integrity monitoring (FIM) controls that monitor for, and reports on file changes and changes to operating systems (OSs) which could indicate compromised systems [80]. FIM controls may also be deployed in a preventative function. The detection phase can also provide an assurance that the technical controls deployed in the protect phase is working properly, and doing what it is supposed to do (namely, rules and filters are working, and attacks and malware are blocked).

## Phase 3: Respond

Phase 3 is initiated once a breach is discovered, and at national and organisational level, this is typically the task of a CERT, or CSIRT [81]. In South Africa, this phase is supported by the Cybersecurity Hub [82] that looks after national interests, and the Electronic Communications Security Computer Security Incident Response Team (ECS-CERT) [83] looking after government interests. A CERT or CSIRT co-ordinates, and supports response to cybersecurity incidents.



The respond phase has its own sub-phases. The SysAdmin, Audit, Networking, and Security (SANS) Institute describes the respond sub-phase as identification, containment, eradication, recovery and lessons learned [84], while NIST lists them as preparation, detection and analysis, containment, eradication and recovery, and post-incident activity [72].

## Phase 4: Recover

This phase starts as part of the “respond” phase, and involves business continuity management (BCM) and the business continuity plan (BCP). BCM is defined as “the capability of the organization to continue delivery of products or services at acceptable predefined levels following a disruptive incident.” [85]. BCM is more holistic than IT disaster recovery in that service and functions are recovered inclusive of the IT, and systems supporting those services and functions. It includes aspects such as people, facilities, telephony and networks.

Although the defensive domain can include sub-domains such as strategic cyber operations [86] and battlefield cyber capabilities, not all of these are applicable to all states and nations [1]. The

application of the NCMF is illustrated in context of the defensive domain and each of the cyber defence lifecycle phases proposed by NATO [1] has its own cybersecurity functions and services, and could be offered from different cybersecurity structures.

The defensive domain also has its own unique actors. These actors may be government actors and may include public actors in the public space. Table 9 shows possible actors interacting with the defensive domain. The actors are South African actors, and we have identified them based on our experience, and using the stakeholders and actor identification template that we proposed in Table 3.8.

**Table 9: Defensive domain lifecycle actors**

| | Government | National | International |
|---|---|---|---|
| **State and Government Actors** | DTPS, SAPS, South African Reserve Bank (SARB), SSA, DOD, DTPS, ECS-CSIRT. | Cybersecurity hub, State Information Technology Agency (SITA), Cybersecurity Hub | **None -** State and government actors by definition exclude International actors. |
| **Organised Non-State Actors** | **None** - Organised non-state actors by definition excludes government. | South African Banking Risk Information Centre (SABRIC) as the financial sector-CSIRT, IT Industry, ISP's fixed and mobile operators, service providers, information security group. | US-CERT, FIRST, Vendors. |
| **Non-Organised Non-State Actors** | **None -** Non-organised non-state actors by definition excludes government. | Public, South African Cyber Security Academic Alliance, Centre for Cybersecurity at UJ, South African Centre for Information Security. | Hacking groups. |

In Section 3.6, we mentioned that the overall purpose for considering the domains is to provide input into the selection and prioritisation of cybersecurity functions, and assist with the identification of cybersecurity structures from where cybersecurity functions could be offered from. We further mentioned that the domains might provide input into the identification of actors.

We have proposed and presented the actor and stakeholder identification template in Table 8. The actor and stakeholder identification template will assist us with the identification of actors across

the three dimensions, and the result is a list of all possible national actors. From this list of actors, some of them will be assigned the responsibility of implementing and managing:

- One or more national cybersecurity functions
- National cybersecurity structures, and,
- Domains.

It would thus be helpful if we had a template that could assist us to map the actors to a cybersecurity function, structure, and domain lifecycle phases. To assist with this, we propose a function, structure and actor identification template for domains in Table 10. This template may be used to map the actors identified in Table 9 as input. Our function, structure and actor identification template for domains may be used to identify lifecycle actors for the defensive as well as the offensive domains.

Table 10 shows an illustrative application of the template. It needs to be noted that the general cybersecurity functions are identified in Chapter 4. It may happen at national level that one function may be offered from a single structure with a single government entity responsible for the function, or a single function may be offered from multiple structures, under the auspices of multiple government entities.

**Table 10: Function, structure and actor identification template for domains**

| | Prevent | Detect | Respond | Recover |
|---|---|---|---|---|
| **National Cybersecurity Function** | Military cyber / cyber warfare | Monitoring and evaluation | Incident handling | Incident handling |
| **Structure** | DOD Cyber Command | SITA | Cybersecurity Hub, ECS-CSIRT | Cybersecurity Hub, ECS-CSIRT |
| **Actors** | DOD | DOD / DTPS / SSA | DTPS / SSA / DOD | SABRIC / CIIP |

This ends our discussion on the defensive domain. Section 3.7 contextualise the cybersecurity domains and actors that were introduced in Section 3.6.1 and Section 3.6.2 for South Africa.

## 3.7 Contextualising the domains and actors

The NCMF actors, and the domains they operate in, are shown in Figure 17, and is contextualised for the South African environment. The figure was taken from NATO [1] and adapted by the author. The figure shows the offensive and defensive domains as described in NATO's National Cybersecurity Framework Manual [1].

Figure 17 is a visual representation of the possible actors in the offensive and defensive domains. The stakeholders and actors identification template presented in Section 3.5.3 in Table 8 was used to populate Figure 17. The actors in the defensive domain are shown in more detail than the actors in the offensive domain since the decision was made and motivated in Section 3.6 to illustrate the application of the NCMF in context of the defensive domain. The three dimensions of government, national and international, with their actors and stakeholders were introduced in Section 3.5. The defensive and offensive domains with their actors is shown in Figure 17.

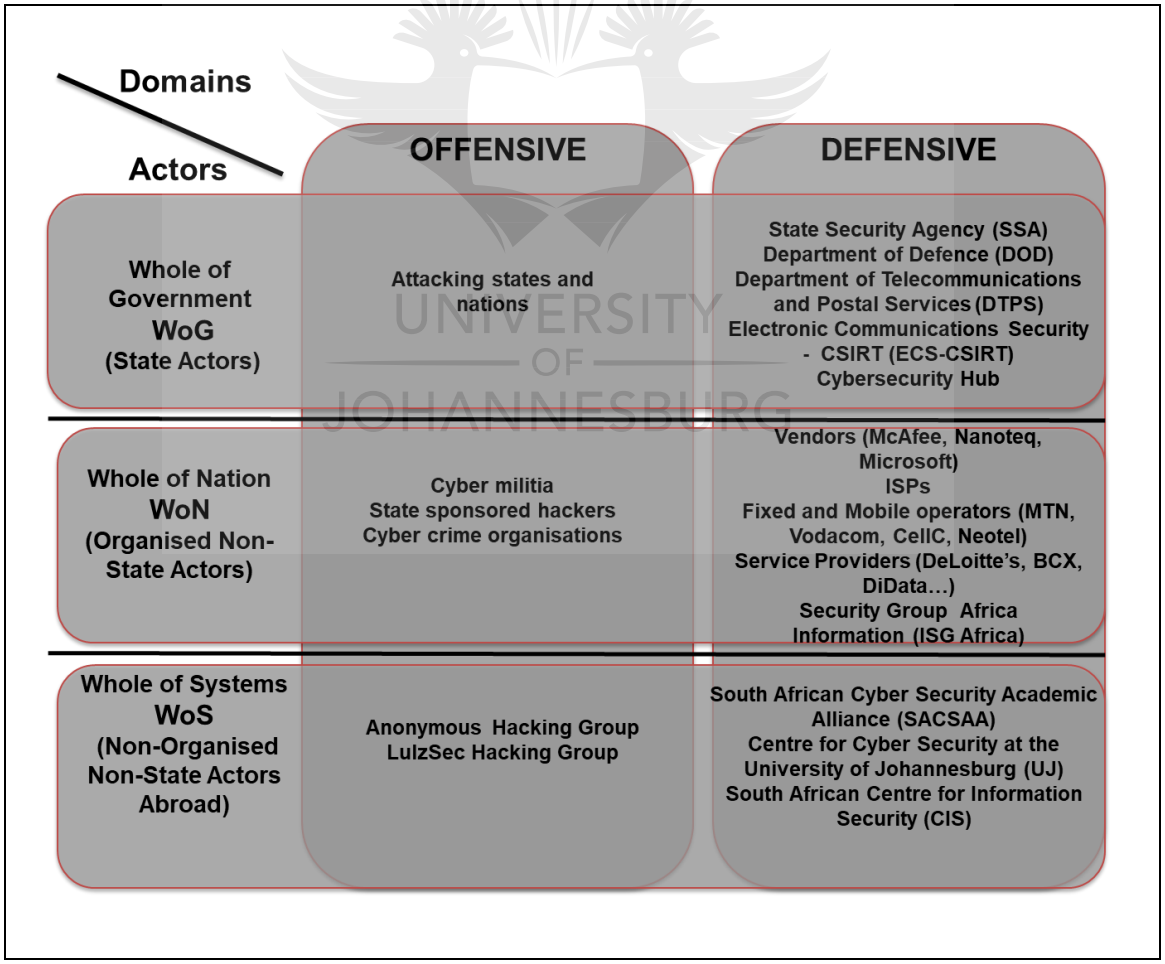



**Figure 17: NCMF actors and associated domains as taken from NATO** [1]**, adapted by the author**

Figure 17 shows that the state and government actors in the defensive activity domain from a South African perspective is the SSA, the DOD, the DTPS, as well as the ECS-CSIRT and the Cybersecurity Hub. The DTPS is an actor acting on the South African national Cybersecurity Hub structure and the SSA is an actor acting on the ECS-CSIRT structure. There will be instances where the state and government actor's responsibilities overlap across the offensive and defensive domains.

An example of overlapping responsibilities is the South African DOD's responsibility to defend South Africa's cyber space in times of peace (defensive domain), but they also have to offer an offensive function during times of war (offensive domain). The selection of a domain for the NCMF to operate in is unique, and specific to the nation state's geo-political posture during the application of the NCMF.

The principle that we want to communicate though, is that it is necessary to select a domain to assist with the identification of cybersecurity structures. Section 3.8 introduces the cybersecurity mandates. Nation states using the NCMF need to select a mandate, or mandates for the NCMF. The cybersecurity mandates influence the identification and selection of national cybersecurity functions.

## 3.8 Cybersecurity mandates

Figure 18 serves to orient the Reader, and shows that this section will be used to discuss the NCMF Mandates. The five Mandates identified by NATO, and displayed in Figure **18** are:



- Military cyber
- Counter cybercrime
- Intelligence and counter-intelligence
- Critical information infrastructure protection (CIIP) and national crisis management
- Cyber diplomacy and internet governance

A mandate is a formal order, or provides someone with the authority to do something, or to behave in a certain way [87]. In the context of the NCMF, the mandate gives the NCMF the authority to act in a specific way during the nation's cybersecurity effort. It also influences the selection and prioritisation of national cybersecurity functions. NATO [1], identified five mandates and these are military cyber, counter cybercrime, intelligence and counter-intelligence, critical information infrastructure protection (CIIP), national crisis management and cyber diplomacy and internet governance.

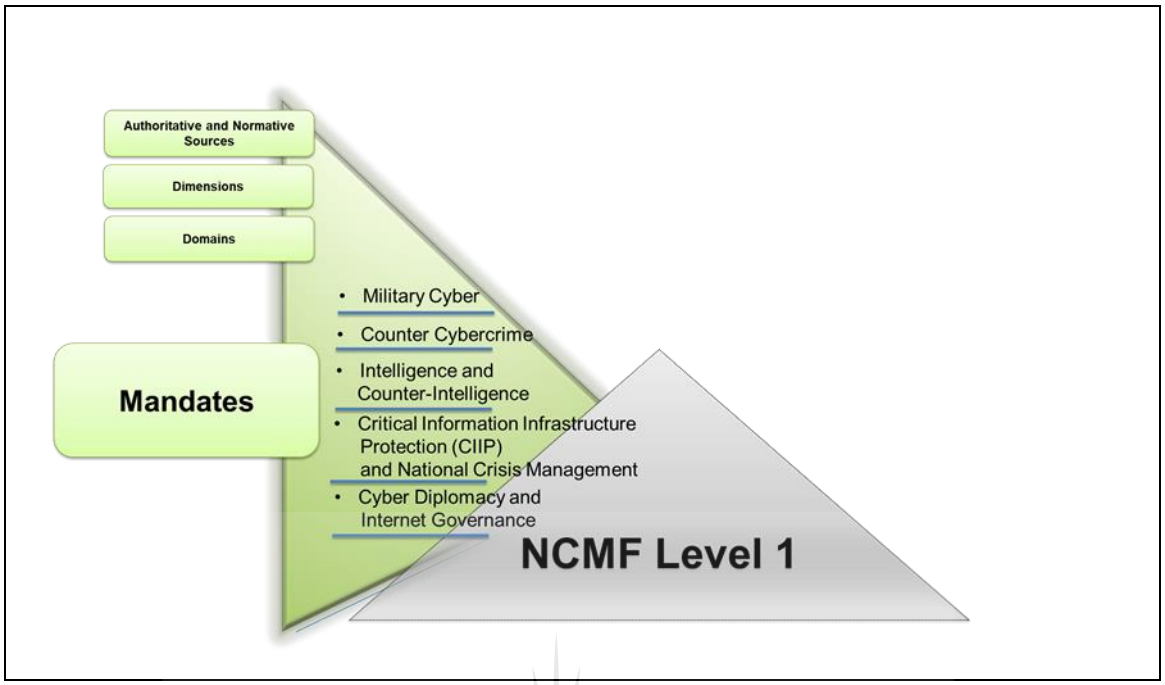



**Figure 18: Section 3.6 Orientation - Mandates**

The NCMF can operate in one, many, or all mandates, and each mandate is the responsibility of a Government department, or one Government department could be responsible for more than one mandate. One or more of the cybersecurity mandates need to be selected for the NCMF. The purpose of the national cybersecurity mandates is to:

- Provide input into the selection and prioritisation of cybersecurity functions. As an example, if a nation selects the military cyber mandate, then actors and functions supporting the mandate will receive priority for implementation.
- Assist nation states to identify responsible actors. Different mandates require different actors.

The five mandates, as taken from NATO [1], and adapted for the South African context, are introduced next.

### 3.8.1 Mandate 1: Military cyber

This mandate forms part of the offensive domain, and as discussed, our focus is on the defensive domain. The military cyber mandate is thus not discussed in detail. This military cyber mandate consists of five services and these are [1]:

- Protection of South African defence networks.
- Establishing a cyber warfare capability.

- Development of a network-centric warfare capability (sensor to shooter, or intelligent logistics).
- Battlefield or tactical cyber warfare, and,
- Strategic cyber-warfare.

In-South Africa, the military cyber mandate is executed by cybersecurity functions and services offered from the DOD Cyber Command, as prescribed by the NCPF [6] and the Cybercrimes and Cybersecurity Bill [34].

### 3.8.2 Mandate 2: Counter cybercrime

Cybercrime happens when criminals exploit the anonymity and speed of the internet to commit crimes across borders. This mandate covers cyberterrorism, theft of identity, and theft of intellectual property. Cybercrime is one of the fastest growing areas of crime globally. The World Economic Forum (WEF) estimates the cost of cybercrime at $445 billion per annum [88]. Interpol distinguishes between two main categories of cybercrime [89].

The first category is advanced cybercrime. This category describes sophisticated attacks against computer systems. The second category is cyber-enabled crime. This is where a traditional crime is enabled by cyber. Examples include crimes against children, terrorism, and financial crime. Since there are no jurisdictional restrictions or boundaries where it concerns cybercrime, collaboration and cooperation between nations is essential. From a South African perspective, this mandate is performed by national cybersecurity functions offered from the SAPS Cybercrime Centre, as mandated by the NCPF [6] and the Cybercrimes and Cybersecurity Bill [34]. The Counter Cybercrime mandate resides in the defensive domain.



### 3.8.3 Mandate 3: Intelligence and counter-intelligence

This mandate prescribes national cybersecurity functions to detect and combat cyber intrusions, and could rely on aspects outside of the cyber domain, such as human-intelligence and signal-intelligence. Specific foreign policy response mechanisms need to be developed to govern intelligence and counter-intelligence in the cyber domain.

This mandate may also include functions to spy on nations. From a South African perspective, this mandate is performed by national cybersecurity functions offered by the State Security Agency (SSA) using various cybersecurity structures, as well as the DOD Cyber Command as prescribed by the NCPF [6] and the Cybercrimes and Cybersecurity Bill.

The Intelligence and Counter-Intelligence mandate resides in both the defensive and offensive domains in that this mandate may be helpful to predict cyber-attacks (see Section 3.6.2). It may also be used in an offensive manner during times of war, to actively spy on nation states.

### 3.8.4 Mandate 4: Critical information infrastructure protection (CIIP) and national crisis management

Critical Information Infrastructure (CII) must be defined and identified and should form part of the national crisis management structure. Mechanisms must be put in place to facilitate the collaboration and dissemination of information between CII service providers South Africa addresses . CIIP in the NCPF [6], the South African Cybercrimes and Cybersecurity Bill [34] and the Protection of Critical Infrastructure Bill [90].

The National Crisis Management mandate-is satisfied through national cybersecurity functions offered from a national SOC or CSIRT structure [1]. The critical information infrastructure protection (CIIP) and the national crisis management mandate resides in the defensive domain.

### 3.8.5 Mandate 5: Cyber diplomacy and internet governance

This mandate covers the promotion of norms and standards for cyber behaviour, as well as the process by which state and non-state actors manage the internet. Internet governance implies non-government, self-regulation and is comprised of the public sector as well as government.



Some examples of organisations are the Internet Architecture Board (IAB) [91] and the Internet Engineering Task Force (IETF) [92]. Their focus in terms of cybersecurity is a preventative one. The cyber diplomacy and internet governance mandate resides in the defensive domain.

## 3.9 Contextualising the dimensions and mandates

Nations applying our NCMF should contextualise the dimensions and mandates for their countries. This contextualisation helps with the identification of actors. The contextualisation also informs the selection and prioritisation of national cybersecurity functions. We illustrate this approach by contextualising the dimensions and mandates for the South African environment. The three dimensions and five mandates contextualised for the South African environment are shown in Figure 19.

Figure 19 was developed using input from NATO [1] and shows the five mandates and three dimensions with its actors specific to South Africa. One, many or all of these mandates can be

assigned to actors present in the government, national or international dimensions. The figure further shows that each mandate can be viewed from a different perspective such as a government, national or international perspectives. Figure 19 is populated with some of the actors we identified using the stakeholders and actor identification template presented in Section 3.5.3 in Table 8, as well as the function, structure and actor identification template for domains in Table 10.

Figure 19 illustrates how responsibility may be assigned to actors for the different mandates. To illustrate the assigning of responsibilities to actors, the responsibility of government and its departments is to coordinate national crisis management efforts, whereas the national responsibility and focus would be to foster cooperation between, and within industries and their sector-CSIRTs. From a South African context, the Justice, Crime Prevention and Security Cluster (JCPS) [93] is responsible for most mandates. The JCPS consists of the Department of Defence and Military Veterans (DOD and DMV); South African Police Service (SAPS); Justice (DOJ) and Correctional Services; Home Affairs (DHA); State Security Agency (SSA) and Finance.

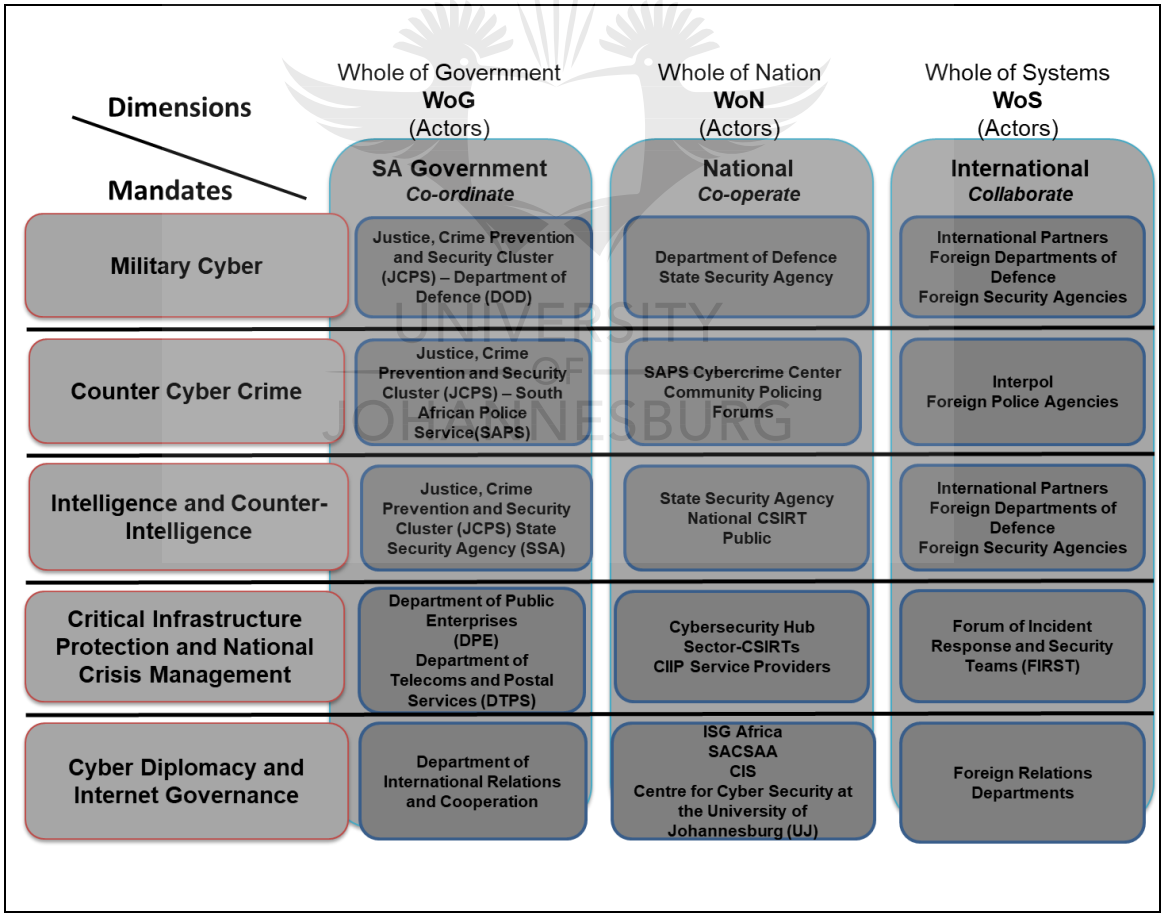



**Figure 19: Mandate actors mapped to dimensions in the South African context** [1]

Figure 19 also illustrates that from a government perspective (Whole of Government) the South African Department of Defence (DOD) is responsible for the military cyber mandate, the South African Police Service is responsible for the counter cybercrime mandate, and the intelligence and counter intelligence mandate is the responsibility of the South African Secret Service (SSA).

Figure 19 further shows that the critical infrastructure protection and national crisis management mandate is the responsibility of the Department of Public Enterprises, and the Department of Telecommunications and Postal Services (DTPS) - who are the state actors at government level. The national Cybersecurity Hub is a state actor at national level, while the sector-CSIRTs are national, non-state actors. FIRST is an international, organised non-state actor.

The cyber diplomacy and internet governance mandate is the responsibility of the South African Department of Justice (DOJ) and the Department of International Relations and Cooperation (DIRCO). It is also shown in Figure 19 that government has a national coordinating function and that non-state actors cooperate at national level. Collaboration takes place at international level, but in essence, the cooperative and collaborative functions need to be managed and facilitated by government.

The responsibilities for the different mandates are assigned in the South African National Cybersecurity Policy Framework (NCPF) [4] and the South African Cybercrimes and Cybersecurity Bill [33]. The state actors, non-state actors and non-state actors abroad may be identified by using the stakeholders and actor identification template introduced in Section 3.5.4, presented in Table 8. The perspective from where the mandates are viewed from, influences the cybersecurity functions required.



The government, with a perspective on coordinating responsibility, might want to implement national cybersecurity crisis management centres to accomplish this (the National Cybersecurity Hub is an example), while at a national level, sector-CSIRTs could be established nationally across sectors and industry to foster cooperation. In terms of international collaboration, the National Cybersecurity Hub and sector-CSIRTs liaise with the Forum of Incident Response and Security Teams (FIRST).

Nations applying the NCMF could select one, or more than one mandate. Each mandate requires a cybersecurity function, or functions. Considering the fiscal and skills constraints, as well as in keeping with the recommendation that developing countries should start small and follow a phased approach during the implementation of national cybersecurity functions, we recommended that developing countries only select one mandate at a time.

The *Critical Infrastructure Protection* and *National Crisis Management* mandate is selected as the mandate in context of which the illustrative application of the NCMF implementation part will be done in Part 2.

## 3.10 Conclusion

Section 3.10 concludes the development of level 1 of the NCMF. In this section, we will provide a summation of the work we have done in Chapter 3, and we then present level 1. The Chapter started with a motivation for the development of a NCMF in Section 3.2. In Section 3.3, the concepts of national and international authoritative and normative sources were introduced. These authoritative sources are of paramount importance, as they will be consulted to identify prescripts for mandatory national cybersecurity functions. National and international normative sources may be used to identify non-mandatory functions.

In sections 3.5 to 3.8, the dimensions, mandates and domains were introduced, and selected to illustrate the application of the NCMF. The NCMF dimensions, mandates and domains assist the user of the NCMF to identify non-mandatory national cybersecurity functions and actors. Section 3.5 introduced the three dimensions of government, national and international.

Each of these dimensions has actors associated with its and some of the actors in the three dimensions were identified in the context of South Africa. The identification of actors is important since responsibility for the application of the NCMF, as well as responsibility for the implementation of national cybersecurity functions will be assigned to them. To assist with the identification of actors, we proposed, and presented a stakeholders and actor identification template in Section 3.5.3 in Table 8.

Section 3.6 introduced the two domains. The two domains are the offensive domain, and the defensive domain. The defensive domain was selected as the domain of operation for the NCMF, and the selection was made based on our work experience in the defensive domain. The defensive domain's four lifecycle phase was introduced. They are the protecting, detecting, responding and recovering phases. Different defensive domain lifecycle phases need different national cybersecurity functions, and national cybersecurity structures. An understanding of the defensive domain lifecycle phases can thus assist with dentifying national cybersecurity structures, the functions and services it offers, and its actors.

The domain selected may also influence the selection of national cybersecurity functions for implementation. To assist with the identification of domain-specific structures and actors we have proposed and presented a function, structure and actor identification template for domains in

Table 10. This template may be populated with the actors identified with the stakeholders and actor identification template in Section 3.5.3 inTable 8. Section 3.8 introduced and discussed the five mandates. The five mandates are military cyber, counter cybercrime, intelligence and counter intelligence, critical information infrastructure protection and national crisis management, and cyber diplomacy and internet governance.

The mandate selected to illustrate application of the NCMF implementation part, is the critical information infrastructure protection, and national crisis management mandates. Our motivation for selecting this mandate, is that we have experience working with these mandates at the national level. Level 1 is presented in Figure 20.

Figure 20 shows that authoritative and normative prescripts and recommendations, dimensions, mandates and domains in which the NCMF operate need to be considered. It also shows that a nation's government is responsible for level 1 of the NCMF. Level 1 of the NCMF is foundational in nature, and if not applied correctly, the identification, selection and prioritisation of national cybersecurity functions might not be relevant to the nation-state applying the NCMF.

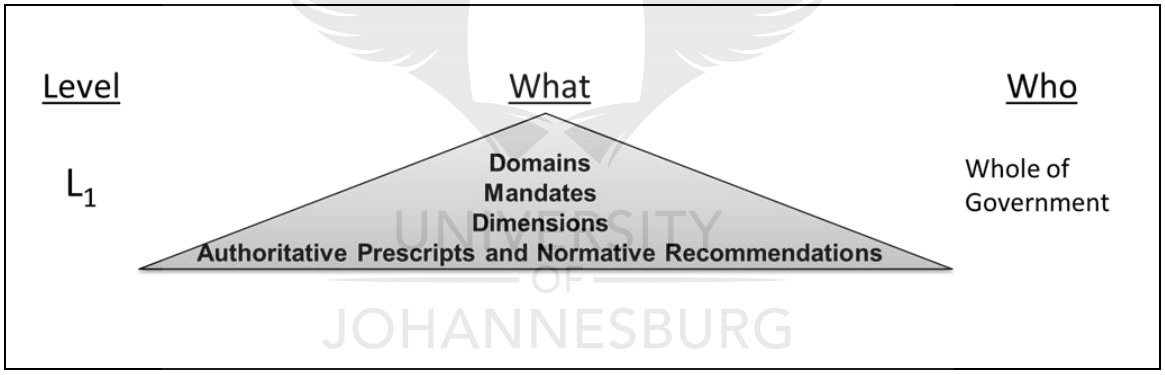


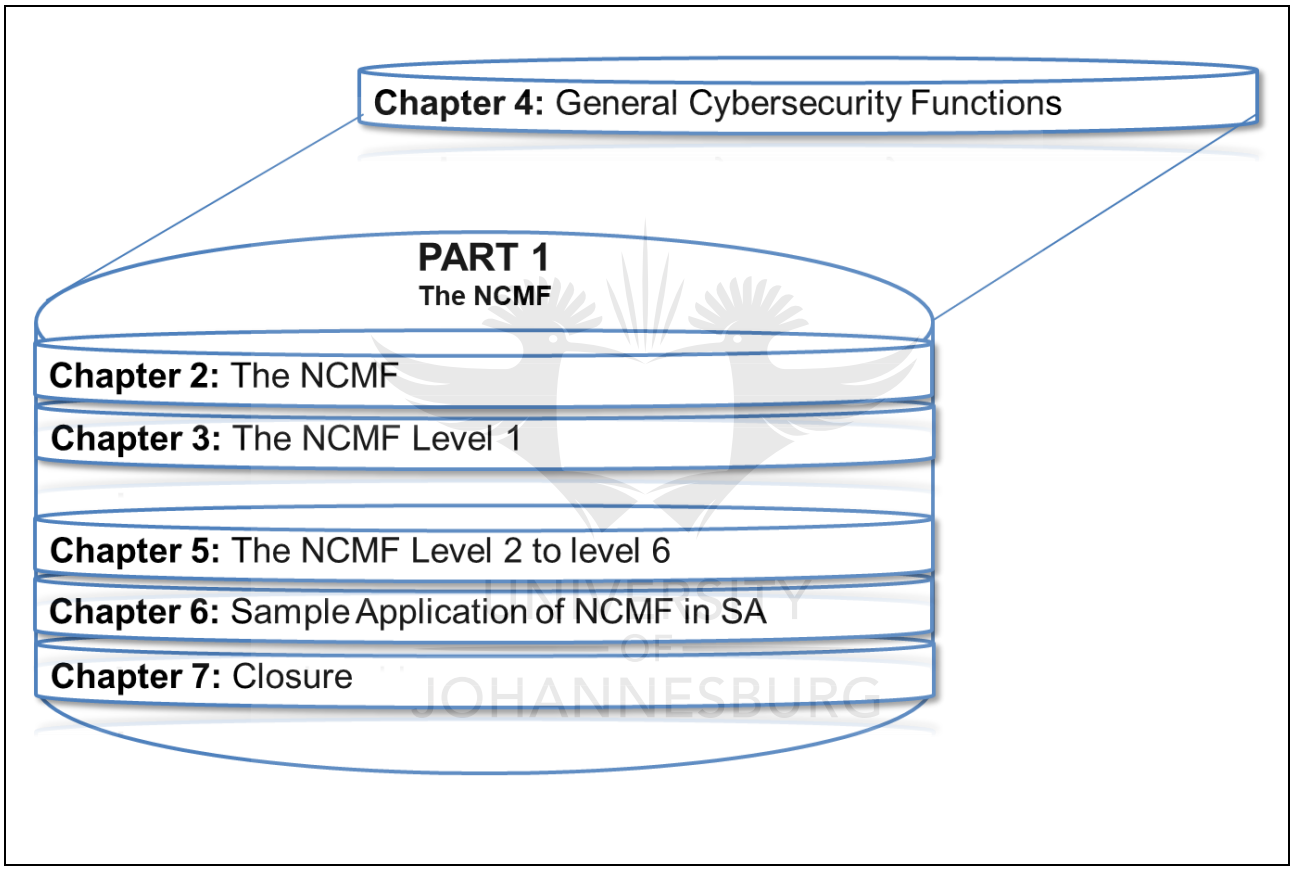



**Figure 20: NCMF Level 1**

Now that we have introduced and discussed level 1 of the NCMF, we will use level 1 in Chapter 4, to identify general cybersecurity functions. We will identify the prescripts in national and international authoritative sources, as well as the recommendations in national and international normative sources. This will result in a list of mandatory and non-mandatory cybersecurity functions. From this list, we will identify the most commonly occurring functions to get to a list of general cybersecurity functions.

It is important to identify and introduce these functions, since some of them will serve as examples during our illustrative application of the rest of the NCMF levels. Chapter 4 is still part of level 1 and identifies and introduces the general cybersecurity functions. This is achieved by building on, and using the level 1 elements discussed in this Chapter. The sole purpose of Chapter 4 is thus to

identify and introduce the general cybersecurity functions. Chapter 4 must be read as being part of the level 1 discussion, and as flowing from Chapter 3.


Chapter 4: General Cybersecurity Functions
PART 1
The NCMF
Chapter 2: The NCMF
Chapter 3: The NCMF Level 1
Chapter 5: The NCMF Level 2 to level 6
Chapter 6: Sample Application of NCMF in SA
Chapter 7: Closure

# Chapter 4: General cybersecurity functions

## 4.1 Introduction

Chapter 4 builds on the introduction and discussion we had of level 1, in Chapter 3. The purpose for the development of our NCMF, is to provide a framework that can assist developed and developing countries with their national cybersecurity management tasks. These tasks were introduced in Section 2.1 as the identification, selection, prioritisation and implementation of national cybersecurity functions. National mandatory or non-mandatory cybersecurity functions are identified at level 1 of the NCMF, and selected and prioritised at level 2 of the NCMF.

Level 1 is used to identify national and international authoritative sources, and from those sources, identify their mandatory cybersecurity function prescripts. Level 1 may also be used to identify non-mandatory cybersecurity functions using general recommendations in national and international normative sources. A nation-state may also select to identify and use existing authoritative sources from other countries, and use the other countries' mandatory functional prescripts as its non-mandatory function recommendation. This means that the authoritative sources of a disparate country become a normative reference for the country using it. We will follow this approach, and use the NCMF's level 1, to identify a list of the most general cybersecurity functions.

In most instances, most developing nations have not yet developed national authoritative sources such as a NCS [94]. They also often lack the capability and capacity to identify national cybersecurity functions themselves. Our general cybersecurity functions will provide these developing countries with a list of predetermined, general cybersecurity functions, and they can select functions from this list for national implementation. The general cybersecurity functions are identified and discussed in more detail here. The two cybersecurity function types were briefly introduced as nation-state specific and mandatory national cybersecurity functions, and non-mandatory cybersecurity functions that are general in nature, and this Chapter builds on the introduction made in Section 3.3.

The purpose of Chapter 4 is to identify and introduce, in more detail, general cybersecurity functions that appear most commonly across the sources we will consult. It is important to have a solid understanding of these functions, their service and complementary capabilities, and the structures from where they are offered. Our intention is to select two of these functions, and then merge their relevant services and capabilities (consisting of people, processes and technology as explained in Section 2.4). These merged services and capabilities will then be offered from a new national cybersecurity structure, called the E-CMIRC (See Part 2 for a best practice guide on how to establish such a structure). This selection must happen in context of developing countries, keeping in mind their constraints and unique requirements. The rest of the Chapter is structured as follows:

**Section 4.2** provides a motivation for the identification of the general cybersecurity functions.

**Section 4.3** presents the aims of the general cybersecurity functions, and illustrates how they can be selected and prioritised by nation states.

**Section 4.4** discusses developing countries, and their constraints in context of national cybersecurity matters.

**Section 4.5** introduces the approach that we have followed to identify a list of general cybersecurity functions.

**Section 4.6** introduces and discusses the general cybersecurity functions. We also select and motivate two of the general cybersecurity functions for use in the development of a new, national cybersecurity structure, the E-CMIRC.

**Section 4.7** concludes the Chapter.

## 4.2 Motivation

National cybersecurity functions can be general (non-mandatory) in nature, or nation-state specific, and mandatory. The NCMF can be used to identify both types. National and international authoritative sources identify the nation-state specific and mandatory, functions. Accordingly, these national and international authoritative sources, together with national and international normative sources may be used to identify non-mandatory functions. The dimensions, domains and mandates inform and influence the selection of cybersecurity functions for implementation. They further assist with the identification of national actors, structures and services.



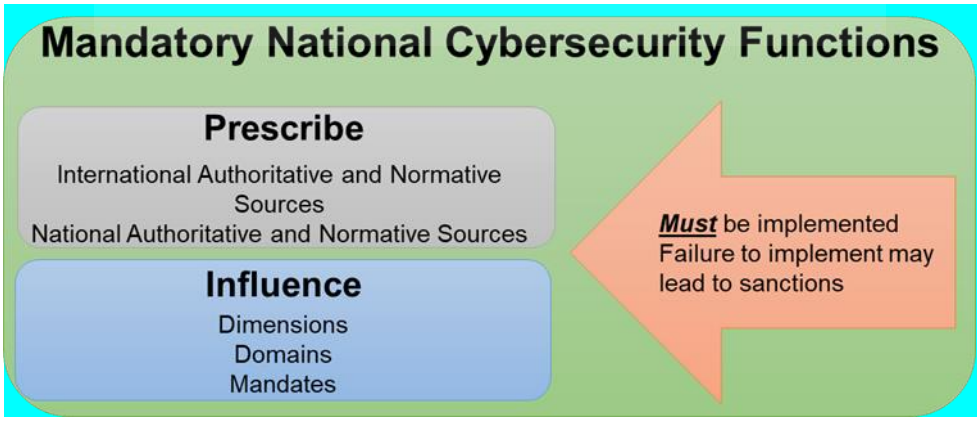



**Figure 21: Mandatory cybersecurity function sources**

The sources used for the identification of mandatory cybersecurity functions are shown in Figure 21 as being national and international authoritative sources, with guidance being provided by the dimensions, mandates and domains. Not implementing these mandatory cybersecurity functions may lead to sanctions.

As with mandatory national cybersecurity functions, the dimensions, domains and mandates influence the selection of non-mandatory cybersecurity functions for implementation, and assist with the identification of actors, structures and functions. Figure 22 shows that the sources used to identify non-mandatory national cybersecurity functions are typically national and international normative sources.

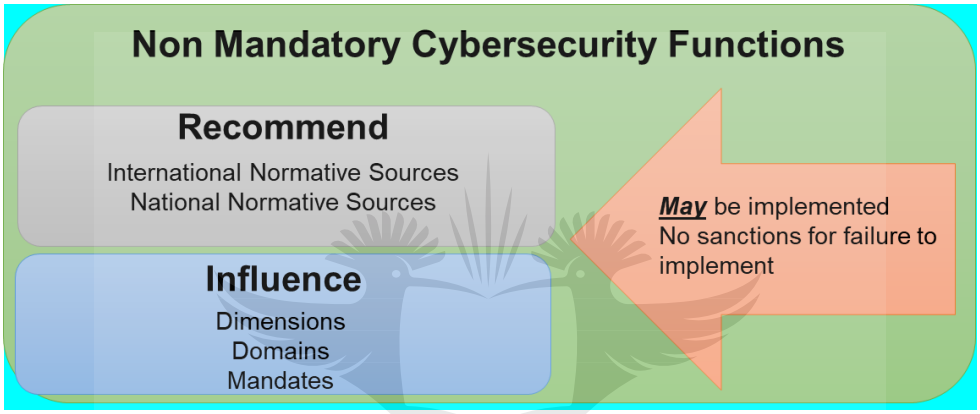



**Figure 22: Non-mandatory cybersecurity function sources**



The cybersecurity functions mentioned in these sources are viewed as recommendations and are not mandatory. We use the term “typically” because nation states may also select to use authoritative sources from other countries to identify cybersecurity functions that they can use as non-mandatory functions for their own countries. We will follow this approach in Chapter 4 where we will use international normative sources as our primary source, but also use national and international authoritative sources to augment our list of functions. Not implementing these cybersecurity functions does not lead to sanctions.

We will be using the NCMF in this chapter to identify the general functions that are most common across the sources we will consult. We have previously stated that the NCMF is developed in the context of developing countries. General cybersecurity functions may be identified by consulting national and international normative sources, and will then formulate the cybersecurity functional recommendations based on them. In keeping with our intention to develop the NCMF in the context of developing countries, South African authoritative sources will also be consulted, and these sources’ cybersecurity function prescripts will be considered for inclusion in our list of general cybersecurity functions. Our approach with regard to identifying the general cybersecurity functions using both authoritative and normative sources is motivated as follows:

- The international normative sources will provide non-mandatory cybersecurity functions, and the South African authoritative sources will provide mandatory cybersecurity functions in the context of a developing country.
- Consulting authoritative and normative sources allows us to illustrate the application of the NCMF to identify not only non-mandatory cybersecurity functions, but also mandatory cybersecurity functions.
- Finding an overlap and appearance of functions across authoritative and normative sources allows some measure of certainty that our functions are general in nature, relevant and applicable to South Africa.
- Similarities between our non-mandatory cybersecurity functions and functions from authoritative sources, gives us the certainty that our non-mandatory functions are aligned with international standards and approaches.

We are following this approach so that we can identify, and then compile a list of general cybersecurity functions, that is not only applicable to developing countries, but is also relevant to developed countries. We will further test the relevancy and accuracy of our general cybersecurity functions by comparing, and identifying similarities between developed countries' authoritative sources. Our focus will, however, be on the identification of the most commonly occurring functions, in other words, the general cybersecurity functions.

Level 1 of the NCMF describes the identification of national authoritative and normative sources. We will thus identify South African national authoritative sources, and consult them to determine mandatory cybersecurity functions. These functions are specific to South Africa. International normative sources will then be identified and consulted to determine international non-mandatory cybersecurity functions. Lastly, international authoritative sources are identified, and our list of non-mandatory functions are then compared against these sources. The most commonly functions are then identified.



Nation states may identify similar, or even totally different cybersecurity functions, and this outcome is determined by the relevant sources they use, as well as their dimensions, mandates and domains. They may even identify many more, or fewer non-mandatory cybersecurity functions than we do. Our list of general cybersecurity functions is thus a fluid list, and subject to change. Our approach further illustrates the effectiveness of the NCMF, as well as its flexibility, in demonstrating that it can be applied by both developed and developing countries.

The identified South African authoritative sources provide input with respect to a developing country. General international normative sources, written by developed countries, will be used to provide input applicable to developed countries. For countries that do not have the capability or capacity to identify their own national cybersecurity functions, the identified non-mandatory cybersecurity functions could serve to provide a "basket," or list of general cybersecurity functions from which they can choose one or two, for implementation.

In Section 4.3, the aims of the general cybersecurity functions are introduced.

## 4.3 Aims of the general cybersecurity functions

The identification of general cybersecurity functions, and the rationale for the presentation of these functions in this Chapter, is done with two aims in mind. These aims are:

- **Aim 1** is to provide a list of pre-determined, non-mandatory cybersecurity functions from which developed and developing countries may make a selection, for implementation. This means that countries that have not yet developed their own authoritative and normative sources, or experience skills and fiscal constraints, do not need to apply level 1 of the NCMF, but can select one or two of the predetermined, non-mandatory functions. Level 1 is applied, when following this approach, by a third party, to identify non-mandatory cybersecurity functions on behalf of the nation-state. Level 1 is thus still used, but applied by a third party, and not by the nation-state using the NCMF.

- **Aim 2:** is for nation states identifying their own national cybersecurity functions, to use this predetermined list of non-mandatory cybersecurity functions against which to measure the strategic relevance and completeness of their own identified national cybersecurity functions. The non-mandatory cybersecurity functions are all strategic in nature, (as opposed to tactical or operational), and, as such, provide a predetermined list of functions that are general in nature, against which to measure the strategic relevance and completeness of their mandatory national cybersecurity functions. The strategic nature of the NCMF will be introduced and described as part of the NCMF implementation strategy in Section I.1.

These two aims are not meant to imply that levels 1 and 2 of the NCMF are of lesser importance, but having a list of non-mandatory cybersecurity functions is helpful in a scenario where there is a lack of authoritative and normative sources. Based on our experience, this is a scenario often found in developing countries. The United Nations (UN) reported in 2017 [95] that only about 38% of nation-states have a published NCSs (an authoritative source), and these are mostly published by developed countries.

It is further advantageous to have the general cybersecurity functions to use as a baseline, or foundation, against which to measure the completeness and relevance of a nation's identified national cybersecurity functions. Being able to measure the national cybersecurity functions against an existing baseline is useful in that it ensures alignment with the international community and its cybersecurity efforts.

In Section 4.4, we will introduce developing countries and their unique requirements briefly with regard to national cybersecurity. We also motivate our recommendation that developing countries should select one, or two cybersecurity functions at a time for implementation, and to follow a phased approach.

## 4.4 Developing countries and national cybersecurity

Our experience has shown that developing countries would benefit the most from a list of predetermined, general and non-mandatory cybersecurity functions. Our experience has further shown, and it is our recommendation, that developing countries should start small, and follow a phased approach, and this means that they should select one, or at most two, of the functions for implementation at national level. This can result in an improvement in their national cybersecurity posture.

In Section 1.1, the statement was made that developing countries have unique requirements concerning its ICT, as well as the securing its ICT at national level. Some differences between developing and developed countries related to their national cybersecurity efforts, are the availability of skills [96] [97]. Developing countries typically have fewer people skilled in cybersecurity, as opposed to developed countries where the skills shortage is not as evident.

Another difference is that developing countries often have less money to spend on national ICT infrastructure development. This impacts negatively on their research infrastructure and cyber-driven commercial activities. Developing countries are also typically burdened with intense foreign debt [98]. National cybersecurity often fails to receive the focus and resource allocation it should, due to the lack of funding for ICT and the skills shortage - both at industrial and national level.

When considering developing countries' skills shortage and financial constraints where it concerns the implementation and securing of its national ICT infrastructure, one can conclude that it will not be feasible for them to implement all the general cybersecurity functions at once. It is our belief that developing countries should start small, and build on their initial successes when implementing national cybersecurity strategy and national cybersecurity functions. In other words, they should follow a structured and phased approach.

Accordingly, developing countries should select and prioritise one or two of the identified general cybersecurity functions to implement strategically – a move which will save costs, and will allow for the identification and skilling of resources to plan, build, run and monitor the national cybersecurity function. The NCMF level 1 is applied in Section 4.6 to identify the most general, non-mandatory cybersecurity functions.

## 4.5 Concepts identifying a list of general cybersecurity functions

In this section, we will introduce the process that we followed during the identification of the general cybersecurity functions. In Section 3.3, where we discussed the NCMF level 1 elements, authoritative and normative sources were introduced. We used our experience with working in the South African (as a developing country) national cybersecurity environment to identify South African national authoritative sources.

In order to identify a list of the most commonly occurring mandatory and non-mandatory functions found in national and international authoritative and normative sources, we had to keep three concepts in mind.

**First concept**: Experience showed that it would be helpful to consult international normative sources to discover non-mandatory cybersecurity functions. The international normative sources are mostly from developed countries where development has already been done in terms of frameworks, standards and best practices. There are also implementation references for the cybersecurity functions mentioned in these normative sources that are applied, and implemented successfully. One such example is the implementation of a national incident handling function using the Forum of Incident Response and Security Teams (FIRST) services framework [99].

**Second concept:** We are developing our framework in the context of developing countries. We have thus decided to identify national cybersecurity functions from the authoritative sources of at least one developing country against which to compare the validity of the non-mandatory functions described in the international normative sources. We have selected South Africa as our reference country since we have experience working in South Africa, and also because it is one of the few developing countries that have developed authoritative sources describing national cybersecurity functions.

**Third concept:** Once we have compiled a list of non-mandatory functions as described in international normative sources, as well as the authoritative sources derived from one developing country, we will validate them against international authoritative sources. These sources are selected randomly to avoid bias. This will then ensure that our list of general functions identified from international normative sources, as well as the authoritative sources of one developing country, also appears in a random selection of other nations' authoritative sources. This will substantiate the general nature of our list of cybersecurity functions.



## 4.6 General cybersecurity functions

The identification of general or non-mandatory cybersecurity functions in this chapter is important, since the services and technologies realising two of these functions will be identified, and combined to be offered from a new structure, called the E-CMIRC. In Section 3.3, we introduced and described the level 1 process to be followed during the identification of nation-state specific and mandatory national cybersecurity functions. The process entails first identifying national and international authoritative sources, and then extracting national cybersecurity function prescripts from those sources.

The dimensions, domains and mandates within which the NCMF will operate, is considered next. To determine the non-mandatory cybersecurity functions, international normative sources and their recommendations have been consulted. We will now introduce the sources that we identified and selected for consultation.

**Identified international normative sources:** We have identified normative sources describing national cybersecurity functions for NATO members, America, and the United Kingdom (UK). From a *developed country* perspective, the following international normative sources were identified, and earmarked for consultation to identify non-mandatory cybersecurity functions. The normative sources from developed countries included in this study are:

- The North Atlantic Treaty Organisation's (NATO) National Cyber Security Framework Manual (2011) [1] that can be found here: goo.gl/oVz7iF,
- The United Kingdom's Cybersecurity Capacity Maturity Model for Nations (CMM) - Revised Edition (2016) [53] that can be found here: goo.gl/p7aMhe,
- The ITU National Cybersecurity Strategy Guide (2011) [100] that can be found here: goo.gl/yF4XBQ,
- Cybersecurity Capability Maturity Model (C2M2) - Version 1.1 (2014) developed by the United States Department of Homeland Security [101] that can be found here: goo.gl/Gu8X7V.

**Identified South African authoritative sources:** From a ***developing country*** perspective, South Africa is used as a reference country. Three authoritative South African were used to identify national cybersecurity functions for developing countries from.

- The National Cybersecurity Policy Framework (NCPF) [6], National Gazette No. 39475, 04 December 2015, Vol. 606 that can be found here: goo.gl/YcH6Qn
- The Cybercrimes and Cybersecurity Bill [34], Government Gazette No. 40487 of 9 December 2016 that can be found here: goo.gl/HiAvSo and
- The Protection of Critical Infrastructure Bill 2017 [90] that can be found here: goo.gl/167QB4.



**Identified international authoritative sources:** The European Union Agency for Network and Information Security (ENISA) provides a list of European Nation States' NCSs [94]. From this list, a random and blind selection was made to do a comparative analysis against, and to correlate our identified non-mandatory security functions against, to ensure its relevance. The following developed countries' and the National Cybersecurity Strategies were randomly selected:

- UK's National Cyber Security Strategy 2016-2021 (2016) [102] that can be found here: https://goo.gl/CuhnGK,
- Irish National Cyber Security Strategy 2015-2017 (2015) [103] that can be found here: https://goo.gl/DwA9wY,
- Cyber Security Strategy for Germany (2011) [104] that can be found here: https://goo.gl/oWkvrB,
- Cyber Security Concept of the Slovak Republic (2015) [105] that can be found here: https://goo.gl/6bNDwq .
- Finland's Cyber Security Strategy (2013) [106] that can be found here: https://goo.gl/RBYXdr

For the identification of the non-mandatory cybersecurity functions, level 1 of the NCMF level is followed as discussed above. This concept is displayed in Figure 23. Figure 23 shows level 1 of the NCMF, and it shows the national and international authoritative and normative sources we will use to identify the general cybersecurity functions. From these sources, we have identified thirteen general cybersecurity functions that are applicable to developed and developing countries. The thirteen non-mandatory cybersecurity functions are presented in Table 11, with a detailed description in the following sections.. The thirteen general cybersecurity functions were identified across all the sources consulted, and explicit as well as implicit references to cybersecurity functions were considered. Some of these cybersecurity functions only appear in one or two of the sources, and some appear across all the consulted sources.

It is important to note that we have omitted the dimensions, mandates and domains as influencing elements. These elements are of relevance during the identification of *nation-state specific* cybersecurity functions. It has no influence where it concerns the *identification* of non-mandatory cybersecurity functions. It will only influence the *selection* and *prioritisation* of mandatory and non-mandatory cybersecurity functions.

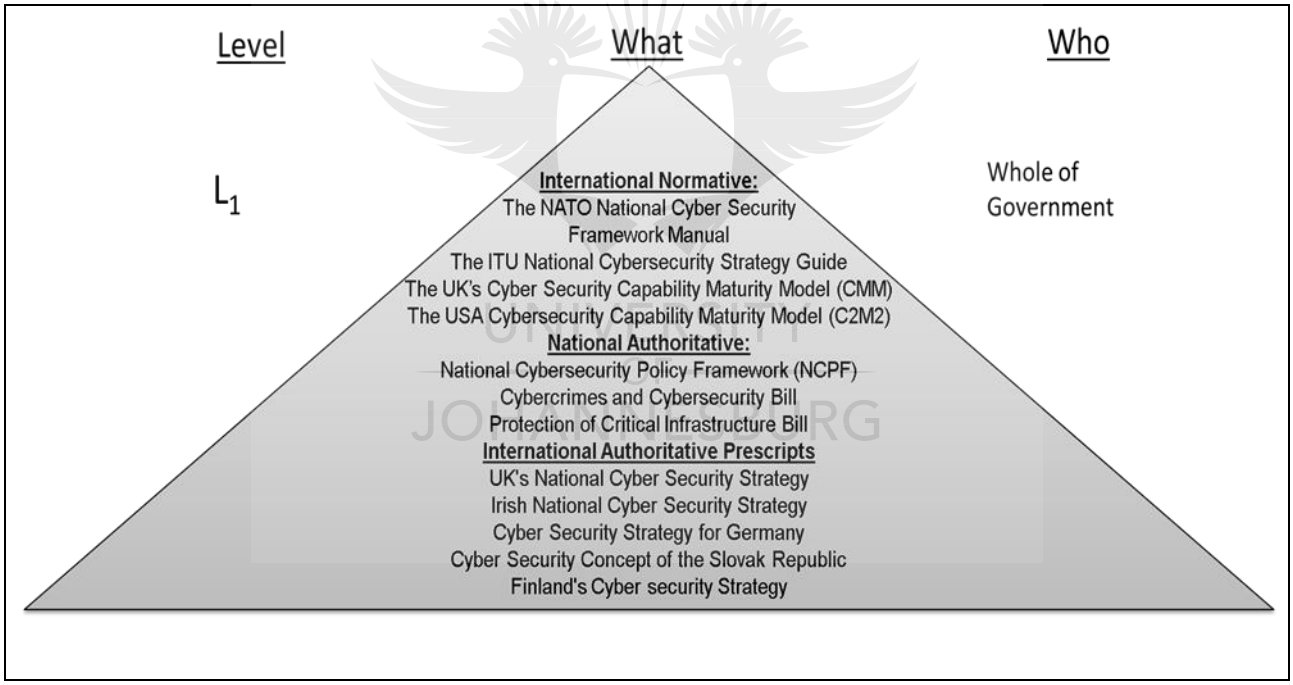



**Figure 23: NCMF Level 1 Non-mandatory cybersecurity functions identification**

Given that the some of the thirteen cybersecurity functions are found across the national and international authoritative and normative sources, for both developed and developing nations, a strong argument can be made that they are general in nature. Some nation states might however require national cybersecurity functions that are not mentioned in the consulted sources. This stems from the fact that the cybersecurity

functional requirements expressed in acts, national cybersecurity policies, and regulatory requirements differ between nations.

Whether or not a nation-state is at war, influences the actors identified across the NCMF dimensions, and it also influences the mandates selected. This, in turn, influences the national cybersecurity functional requirements. Emerging technologies and the adoption thereof (such as the Internet of Things (IoT)) [107] is another factor that may influence a nation's cybersecurity function requirements. For example, the adoption of IoT introduces new technologies, connectivity requirements, communication protocols, and new cyber risks. The adoption of IoT may influence national cybersecurity function requirements in terms of research and development for security controls for IoT, Critical infrastructure providers uses IoT to monitor and manage systems, and new functions may need to be developed to monitor and evaluate IoT.

Considering all the possible elements that may influence the identification, selection and prioritisation of national cybersecurity functions, the necessity of our NCMF guiding nation-states in the identification of applicable national cybersecurity functions - keeping authoritative and normative prescripts, as well as the dimensions, mandates and domains it addresses, in consideration - is emphasised. Once the cybersecurity functions are identified, they also need to be implemented. The identification and consultation of all the elements that determine, inform, and influence national cybersecurity functions also underscore the need for a framework that nation-states can follow to guide them during the implementation of national cybersecurity functions. A best practice implementation guide for national cybersecurity structures can be found in Part 2. Table 11 presents our thirteen general cybersecurity functions that we have identified from the sources shown in Figure 23, with a more detailed discussion in the following sections.



**Table 11: Thirteen general cybersecurity functions**

| sn | General Cybersecurity Function | Section |
|---|---|---|
| 1 | Military cyber / Cyber warfare | 4.6.1 |
| 2 | Cybercrime / Investigations / Digital forensics | 4.6.2 |
| 3 | Research and development (R&D), education and awareness | 4.6.3 |
| 4 | Critical information infrastructure protection (CIIP) | 4.6.4 |
| 5 | Cryptography | 4.6.5 |
| 6 | E-Identity | 4.6.6 |
| 7 | Incident handling | 4.6.7 |
| 8 | Monitoring and evaluation | 4.6.8 |
| 9 | Internal coordination | 4.6.9 |
| 10 | External stakeholder engagement | 4.6.10 |
| 11 | National policy and strategy development | 4.6.11 |
| 12 | National regulations development | 4.6.12 |
| 13 | National strategic risk and threat assessment | 4.6.13 |

The thirteen identified general cybersecurity functions are now discussed in more detail in the text following, and they are presented in the context of South Africa. The non-mandatory functions identified from the international normative sources are introduced, together with their correlated international authoritative sources. The non-mandatory cybersecurity function types are displayed in tables, with the sources where they appear.

### 4.6.1 Military cyber / cyber warfare

Table 12 introduces the military cyber function. This cybersecurity function refers to the capability of South Africa to engage in cyber warfare, where cyber warfare is defined as the actions of a nation state to "penetrate another nations' computers or networks for the purposes of causing damage or disruption" [108]. This national cybersecurity function provides South Africa with a military cyber offensive and defensive function, to support operational tasks, assist in accomplishing strategic missions, and facilitating a network-centric warfare capability. In South Africa, this function is enabled or realised by services offered from the DOD Cyber Command structure.

**Table 12: Military cyber / cyber warfare**

| Type | General cybersecurity function source | Source document location |
|---|---|---|
| **International normative** | The North Atlantic Treaty Organisation's (NATO) National Cyber Security Framework Manual (2011) [1] | 4.5.1 p121 |
| | The United Kingdom's Cybersecurity Capacity Maturity Model for Nations (CMM) - Revised Edition (2016) [53] | D.1.1 p23 |
| | The ITU National Cybersecurity Strategy Guide (2011) [100] | 7.2 p42 |
| **National authoritative** | The National Cybersecurity Policy Framework (NCPF) [6], National Gazette No. 39475, 04 December 2015, Vol. 606 | 16.5 p94 |
| | The Cybercrimes and Cybersecurity Bill [34], Government Gazette No. 40487 of 9 December 2016 | Ch 6 Section 55 |
| **International authoritative** | UK's National Cyber Security Strategy 2016-2021 (2016) [102] | 1.10; 6.3; 6.5.3 |
| | Irish National Cyber Security Strategy 2015-2017 (2015) [103] | 5.7 p14 |
| | Finland's Cyber Security Strategy (2013) [106] | (5) p8 |

### 4.6.2 Cybercrimes / investigations / digital forensics

Table 13 introduces the cybercrimes, cyber investigations and digital forensics function. This function refers to the capability to investigate and prosecute cybercrimes. Investigations will likely require the ability to perform

digital forensics to obtain evidence for prosecution. This function allows South Africa to develop strategies to govern the development of cybercrime legislation that should be globally applicable and interoperable with the existing national and regional legislation. It further defines the cybersecurity services and capabilities supporting the cybercrime function, such as digital forensics and cybercrime.

**Table 13: Cybercrimes / investigations / digital forensics**

| Type | General Cybersecurity Function Source | Source Document Location |
|---|---|---|
| **International normative** | The North Atlantic Treaty Organisation's (NATO) National Cyber Security Framework Manual (2011) [1] | 4.5.2 p122 |
| | The United Kingdom's Cybersecurity Capacity Maturity Model for Nations (CMM) - Revised Edition (2016) [53] | D.4.3 p47 |
| | The ITU National Cybersecurity Strategy Guide (2011) [100] | 1.4 (4); 11.5 p67 |
| **National authoritative** | The National Cybersecurity Policy Framework (NCPF) [6], National Gazette No. 39475, 04 December 2015, Vol. 606 | 7 (d) p6; 8 p7; 16.3 p28 |
| | The Cybercrimes and Cybersecurity Bill [34], Government Gazette No. 40487 of 9 December 2016 | Ch 6 Section 54 |
| **International authoritative** | UK's National Cyber Security Strategy 2016-2021 (2016) [102] | 3.2; 3.3; 3.6; Section 4 p28; 6.2 p47 |
| | Irish National Cyber Security Strategy 2015-2017 (2015) [103] | 5.6 p14 |
| | Cyber Security Strategy for Germany (2011) [104] | (6) p6 |
| | Finland's Cyber Security Strategy (2013) [106] | (4) p8 |



### 4.6.3 Research and development (R&D), education and awareness

Table 14 introduces the research and development, education and awareness function. This function describes the South African capability to perform its own independent research and development (R&D) in the field of cybersecurity. The Council for Scientific and Industrial Research (CSIR) is currently involved in helping the DST define an R&D agenda [109]. It also refers to the capability of South Africa to produce individuals that are educated enough to enable and support all the national cyber defence functions that have been identified.

It further refers to the capability to make organisations and individual citizens aware of cybersecurity related issues. This function ensures that all South African stakeholders and actors understand cyber risks, trends

and countermeasures. It also ensures that cyber education and training is available at national level, and institutions are in place to facilitate R&D of cybersecurity at national level.

**Table 14: Research and development (R&D), education and awareness**

| Type | General cybersecurity function source | Source Document Location |
|---|---|---|
| **International Normative** | The North Atlantic Treaty Organisation's (NATO) National Cyber Security Framework Manual (2011) [1] | 4.6.3 p133 |
| | The United Kingdom's cybersecurity capacity maturity model for nations (CMM) - Revised edition (2016) [53] | D.3.2 p 35 |
| | The ITU National cybersecurity strategy guide (2011) [100] | 5.3.8 p30; 18.3.1.1 p90 |
| **National Authoritative** | The National Cybersecurity Policy Framework (NCPF) [6], National Gazette No. 39475, 04 December 2015, Vol. 606 | 1.6 p11; 2.8 p131.1 p15; 5.3.6 (f) p16; 12 p24 |
| | The Cybercrimes and Cybersecurity Bill [34], Government Gazette No. 40487 of 9 December 2016 | 51 (c)(6)(g)(vi) |
| **International Authoritative** | UK's National Cyber Security Strategy 2016-2021 (2016) [102] | 7.0.2 p55; 7.3 p59 |
| | Irish National Cyber Security Strategy 2015-2017 (2015) [103] | 5.12 p16 |
| | Cyber security strategy for Germany (2011) [104] | (8) p7 |
| | Cyber Security Concept of the Slovak Republic (2015) [105] | 3.7 p18 |
| | Finland's Cyber Security Strategy (2013) [106] | (7) p5 |



### 4.6.4 Critical information infrastructure protection (CIIP)

Table 15 introduces the critical infrastructure protection function. This function describes the capability of the country to protect critical ICT or ICT-dependent national infrastructure from threats. Critical infrastructure can be considered any infrastructure that is essential for the functioning of society or the economy [34] [33] [90]. This provides South African critical infrastructure owners, providers and operators with the capability to defend their infrastructure and information against cyber-attacks.

**Table 15: Critical information infrastructure protection (CIIP)**

| Type | General Cybersecurity Function Source | Source Document Location |
|---|---|---|
| **International Normative** | The North Atlantic Treaty Organisation's (NATO) National Cyber Security Framework Manual (2011) [1] | 1.5.2 p36 |
| | The United Kingdom's Cybersecurity Capacity Maturity Model for Nations (CMM) - Revised Edition (2016) [53] | D.1.3 p20 |
| | The ITU National Cybersecurity Strategy Guide (2011) [100] | 1.5.3 p7; 5.1 p25 |
| | Cybersecurity Capability Maturity Model (C2M2) - Version 1.1 (2014) developed by the United States Department of Homeland Security [101] | 2.2 p3 |
| **National Authoritative** | The National Cybersecurity Policy Framework (NCPF) [6], National Gazette No. 39475, 04 December 2015, Vol. 606 | 16.2.1 (e) p27; 19.1 (c) p30 |
| | The Cybercrimes and Cybersecurity Bill [34], Government Gazette No. 40487 of 9 December 2016 | Section 8 Ch 7 |
| | The Protection of Critical Infrastructure Bill 2017 [90] | The whole Bill covers Critical Infrastructure |
| **International Authoritative** | UK's National Cyber Security Strategy 2016-2021 (2016) [102] | 5.4 p39 |
| | Irish National Cyber Security Strategy 2015-2017 (2015) [103] | 2.5 p6 |
| | Cyber Security Strategy for Germany (2011) [104] | (1) p3 |
| | Cyber Security Concept of the Slovak Republic (2015) [105] | 2.2 p6 |



### 4.6.5 Cryptography

Table 16 introduces the cryptography function. This function describes the capability of South Africa to develop and deploy its own cryptographic technology independently. South Africa is provided with its own internal services and capabilities to develop secure cryptographic products and algorithms. The South African Communications Security Agency (SACSA), are incorporated into SSA, and provides the cybersecurity services to realise the Cryptography cybersecurity function [110].

**Table 16: Cryptography**

| Type | General Cybersecurity Function Source | Source Document Location |
|---|---|---|
| **International Normative** | The United Kingdom's Cybersecurity Capacity Maturity Model for Nations (CMM) - Revised Edition (2016) [53] | D.5.5 p56 |
| | The ITU National Cybersecurity Strategy Guide (2011) [100] | 5.3.1 p28 |
| **National Authoritative** | The National Cybersecurity Policy Framework (NCPF) [6], National Gazette No. 39475, 04 December 2015, Vol. 606 | (9) p21 |
| **International Authoritative** | UK's National Cyber Security Strategy 2016-2021 (2016) [102] | 6.6 p51 |

### 4.6.6 E-Identity

Table 17 introduces the e-identity cybersecurity function. This cybersecurity function describes the capability to develop and deploy electronic means to identify and authenticate citizens [6]. This capability provides for the development of a national strategy for developing a generic and universal digital identity system for South African citizens.

**Table 17: E-Identity**

| Type | General cybersecurity function source | Source document location |
|---|---|---|
| **International normative** | The ITU National Cybersecurity Strategy Guide (2011) [100] | 4.3.6 (5) |
| | Cybersecurity Capability Maturity Model (C2M2) - Version 1.1 (2014) developed by the United States Department of Homeland Security [101] | 5.3 p25 |
| **National authoritative** | The National Cybersecurity Policy Framework (NCPF) [6], National Gazette No. 39475, 04 December 2015, Vol. 606 | 10.3 p87 |
| **International authoritative** | UK's National Cyber Security Strategy 2016-2021 (2016) [102] | 5.2.3 p36 |

### 4.6.7 Incident handling

Table 18 introduces the incident handling function. This function deals with the capability of South Africa to respond to cybersecurity-related incidents - such as attacks - in a coordinated and efficient manner. This capability provides incident handling support at a national level. This capability is typically facilitated by a national CSIRT structure. The *incident handling* cybersecurity function is the first national cybersecurity function selected to be offered from the E-CMIRC structure. The rationale for selecting this cybersecurity function is that this is a requirement expressed across all sources consulted as a national cybersecurity

function. A secondary motivation is that we have experience in planning, building, running and monitoring organisational and national CSIRTs. The CSIRT is the structure used to enable or realise the *Incident Handling* function through its cybersecurity services and capabilities.

**Table 18: Incident handling**

| Type | General cybersecurity function source | Source document location |
|---|---|---|
| **international normative** | The North Atlantic Treaty Organisation's (NATO) National Cyber Security Framework Manual (2011) [1] | 4.5.4 p124 |
| | The United Kingdom's Cybersecurity Capacity Maturity Model for Nations (CMM) - Revised Edition (2016) [53] | D.1.2 p17 |
| | The ITU National Cybersecurity Strategy Guide (2011) [100] | 11.3 p64 |
| | Cybersecurity Capability Maturity Model (C2M2) - Version 1.1 (2014) developed by the United States Department of Homeland Security [101] | 5.7 p35 |
| **National authoritative** | The National Cybersecurity Policy Framework (NCPF) [6], National Gazette No. 39475, 04 December 2015, Vol. 606 | 5.3.3 p81; 5.3.5 p81; 5.4 p81 |
| | The Cybercrimes and Cybersecurity Bill [34], Government Gazette No. 40487 of 9 December 2016 | Section 53 Ch 6 |
| **International authoritative** | UK's National Cyber Security Strategy 2016-2021 (2016) [102] | 5.6 p44 |
| | Irish National Cyber Security Strategy 2015-2017 (2015) [103] | 2.6 p7 |
| | Cyber Security Strategy for Germany (2011) [104] | (4) p4 |
| | Cyber Security Concept of the Slovak Republic (2015) [105] | 3.1 p11 - 14 |
| | Finland's Cyber Security Strategy (2013) [106] | (2) p7 |



### 4.6.8 Monitoring and evaluation

Table 19 introduces the monitoring and evaluation function. This cybersecurity function refers to the capability to continuously monitor and evaluate the state of ICT within South Africa in order to detect malicious activity or faults. This is closely related to incident management since many incidents will be detected through the ability to monitor and evaluate ICT.

This capability allows for the monitoring, evaluation and improvement of national cybersecurity services and capabilities, and their effectiveness and performance. The *Monitoring and Evaluation* function is the second cybersecurity function selected to be offered from the E-CMIRC.

**Table 19: Monitoring and evaluation**

| Type | General Cybersecurity Function Source | Source Document Location |
|---|---|---|
| **International normative** | The North Atlantic Treaty Organisation's (NATO) National Cyber Security Framework Manual (2011) [1] | 4.5.2 p122 Compliance function p 177 |
| | The United Kingdom's Cybersecurity Capacity Maturity Model for Nations (CMM) - Revised Edition (2016) [53] | D.1.2 p19; D.5.4 p55 |
| | The ITU National Cybersecurity Strategy Guide (2011) [100] | 2.4.1.1 p15 |
| | Cybersecurity Capability Maturity Model (C2M2) - Version 1.1 (2014) developed by the United States Department of Homeland Security [101] | 5.1 p19; 5.4 p27 |
| **National authoritative** | The National Cybersecurity Policy Framework (NCPF) [6], National Gazette No. 39475, 04 December 2015, Vol. 606 | 7 (c) p71; 16.2.1 (e) |
| | The Cybercrimes and Cybersecurity Bill [34], Government Gazette No. 40487 of 9 December 2016 | 60(3) p110 |
| **International authoritative** | UK's National Cyber Security Strategy 2016-2021 (2016) [102] | 5.0.2 p33; 6.4.4 p50 |
| | Irish National Cyber Security Strategy 2015-2017 (2015) [103] | 5.2 p13 |
| | Cyber Security Strategy for Germany (2011) [104] | (4) p5 |
| | Cyber Security Concept of the Slovak Republic (2015) [105] | 3.1 p12; 3.3 (2) p16 |
| | Finland's Cyber Security Strategy (2013) [106] | (3) p8 |



### 4.6.9 Internal coordination

Table 20 introduces the internal coordination function. This cybersecurity function refers to the internal coordination between government actors responsible for the other cybersecurity functions and services in the framework. This coordination is required to ensure that all the cybersecurity functions and services are being governed, aligned with one another, and executed in accordance with government policy and legislation.

This function allows for the coordination of cybersecurity activities at national level. It also coordinates the national cybersecurity risk assessment, and aligns with CIIP. It further assists with incident and crisis management, and international cybersecurity incidents that involves international stakeholders and actors. The NCMF prescribes the establishment of the overall controlling body in Chapter 3 that will perform this function.

**Table 20: Internal coordination**

| Type | General Cybersecurity Function Source | Source Document Location |
|---|---|---|
| **International normative** | The North Atlantic Treaty Organisation's (NATO) National Cyber Security Framework Manual (2011) [1] | 4.6.1 p130 |
| | The United Kingdom's Cybersecurity Capacity Maturity Model for Nations (CMM) - Revised Edition (2016) [53] | D.1.2 p14; D.1.5 p15 |
| | The ITU National Cybersecurity Strategy Guide (2011) [100] | 4.3.5; 4.3.6 p21 |
| | Cybersecurity Capability Maturity Model (C2M2) - Version 1.1 (2014) developed by the United States Department of Homeland Security [101] | (3) p57 |
| **National authoritative** | The National Cybersecurity Policy Framework (NCPF) [6], National Gazette No. 39475, 04 December 2015, Vol. 606 | 16.5; 16.6 p94 |
| | The Cybercrimes and Cybersecurity Bill [34], Government Gazette No. 40487 of 9 December 2016 | 54 (4)(a) and (c) p90 |
| | The Protection of Critical Infrastructure Bill 2017 [90] | 2 (j) p12; 9 (2)(b) p20 |
| **International authoritative** | UK's National Cyber Security Strategy 2016-2021 (2016) [102] | 4.16 p28 |
| | Cyber Security Strategy for Germany (2011) [104] | p3; p5 |
| | Cyber Security Concept of the Slovak Republic (2015) [105] | 2.2 p6; 3.2(1) p15 |
| | Finland's Cyber Security Strategy (2013) [106] | (1) p7 (3) p4; (10) p11 |



### 4.6.10 External stakeholder engagement

Table 21 introduces the external stakeholder engagement function. This function describes the capability to interact with external, non-government actors, such as local industry representatives, citizens, amongst others,as well as foreign organisations with similar responsibilities in their respective countries. This capability builds relations with foreign stakeholders and actors to facilitate cooperation where it concerns national cybersecurity functions.

**Table 21: External stakeholder engagement**

| Type | General Cybersecurity Function Source | Source Document Location |
|---|---|---|
| **International normative** | The North Atlantic Treaty Organisation's (NATO) National Cyber Security Framework Manual (2011) [1] | 5.4.2 p185 |
| | The United Kingdom's Cybersecurity Capacity Maturity Model for Nations (CMM) - Revised Edition (2016) [53] | (II)(b) p8; D.1.1 p17 |
| | The ITU National Cybersecurity Strategy Guide (2011) [100] | 11.3 p64 |
| **National authoritative** | The National Cybersecurity Policy Framework (NCPF) [6], National Gazette No. 39475, 04 December 2015, Vol. 606 | 11 p23; 4.1.3 p80 |
| | The Cybercrimes and Cybersecurity Bill [34], Government Gazette No. 40487 of 9 December 2016 | 26 p38; 44(2)(b) p61 |
| **International authoritative** | UK's National Cyber Security Strategy 2016-2021 (2016) [102] | 5.0.1 p33; 8.2 p63 |
| | Cyber Security Strategy for Germany (2011) [104] | p2; p3 |
| | Cyber Security Concept of the Slovak Republic (2015) [105] | 3.6 p18 |
| | Finland's Cyber Security Strategy (2013) [106] | (4) and (6) p5; (4) p8; (6) p9 |

### 4.6.11 National policy and strategy development



Table 22 introduces the national policy and strategy development function. This function refers to the capability to develop national policy and strategy around cybersecurity. This capability enables South Africa to develop its own cybersecurity strategy and policy based on, and aligned with international best practices. The National Policy and Strategy Development function could collaborate with the R&D, Education and Awareness function, but this does not necessarily mean that these two functions need to be selected together.

We made the statement in section 2.6 that one of a nation's most important authoritative sources, is its national cybersecurity strategy (NCS). This makes the national policy and strategy development function an important one, and should be considered for early implementation when selecting and prioritising national cybersecurity functions for implementation.

**Table 22: National policy and strategy development**

| Type | General cybersecurity function source | Source Document Location |
|---|---|---|
| **International normative** | The North Atlantic Treaty Organisation's (NATO) National Cyber Security Framework Manual (2011) [1] | 3.4.2 p91; 3.6 p103 |
| | The United Kingdom's Cybersecurity Capacity Maturity Model for Nations (CMM) - Revised Edition (2016) [53] | D.1.1 p16 |
| | The ITU National Cybersecurity Strategy Guide (2011) [100] | 4.3.6 (2) p21; 6 p35 |
| | Cybersecurity Capability Maturity Model (C2M2) - Version 1.1 (2014) developed by the United States Department of Homeland Security [101] | 3.1 p6 |
| **National authoritative** | The National Cybersecurity Policy Framework (NCPF) [6], National Gazette No. 39475, 04 December 2015, Vol. 606 | 5.4.6 p82; 7 (b) p71; 8.2 p85 |
| | The Cybercrimes and Cybersecurity Bill [34], Government Gazette No. 40487 of 9 December 2016 | 51(6)(h) p79; 52(5)(f) p81 |
| | The Protection of Critical Infrastructure Bill 2017 [90] | 7(a)(v) p18 |
| **International authoritative** | UK's National Cyber Security Strategy 2016-2021 (2016) [102] | 7.4.1 p60; 7.4.2 p60 |
| | Irish National Cyber Security Strategy 2015-2017 (2015) [103] | 2.6 p8 |
| | Cyber Security Concept of the Slovak Republic (2015) [105] | 3.1 p12; 3.3(2) p16; 3.6 p18 |

### 4.6.12 National regulations development

Table 23 introduces the national regulations development function. This function describes the capability to create compulsory cybersecurity regulations – at national level – that organisations within the public sector have to adhere to. These regulations specify what individual organisations are required to do to ensure cybersecurity.

Organisational ICT governance frameworks must be used to develop the regulations (such as COBIT and ISO/IEC 27001:2005). The SSA is primarily responsible for developing these regulations from a South African perspective. This cybersecurity function could use as input, and collaborate with the R&D, education and awareness capability, but it is not necessary for them to be selected together.

**Table 23: National regulations development**

| Type | General cybersecurity function source | Source document location |
|---|---|---|
| **International normative** | The North Atlantic Treaty Organisation's (NATO) National Cyber Security Framework Manual (2011) [1] | 4.3 p115; 4.6.1 p131 |
| | The United Kingdom's Cybersecurity Capacity Maturity Model for Nations (CMM) - Revised Edition (2016) [53] | D.4.1 p39 |
| | The ITU National Cybersecurity Strategy Guide (2011) [100] | 9.1.3 p50; 11.4.1 p66 |
| **National authoritative** | The National Cybersecurity Policy Framework (NCPF) [6], National Gazette No. 39475, 04 December 2015, Vol. 606 | 7.1 (c) p84; 8.2 (a) p85; 16.4 (a) 93 |
| | The Cybercrimes and Cybersecurity Bill [34], Government Gazette No. 40487 of 9 December 2016 | 52 (6) p82; All sections talk about regulations |
| | The Protection of Critical Infrastructure Bill 2017 [90] | Ch 6 p46 |
| **International authoritative** | UK's National Cyber Security Strategy 2016-2021 (2016) [102] | 4.16 p27; 5.4.8 p41 |
| | Irish National Cyber Security Strategy 2015-2017 (2015) [103] | (3) p 10; (4) p11 |
| | Cyber Security Concept of the Slovak Republic (2015) [105] | (1) p5; (3) p10 |
| | Finland's Cyber Security Strategy (2013) [106] | (2) p7 |



### 4.6.13 National strategic risk and threat assessment

Table 24 introduces the national strategic risk and threat assessment function. This function deals with the capability to identify risks and threats at a national, strategic level. At a strategic level such risks are not technical cybersecurity risks, but may, for example, be related to geopolitical threats that increase the risk to South Africa's cybersecurity. The rationale for including this function is based on the following two reasons:

- Best practice for cybersecurity governance suggests a risk-based approach [48] [49].
- Risks change over time and, in order for South Africa to adapt as needed, there needs to be a formal, periodic assessment of risks and threats.

This function allows for the establishment, operation and maintenance of a cybersecurity risk management process at national level. This process would serve as input to, and guide the selection and prioritisation of

national cybersecurity functions identified in level 1. We have placed this function at level 2 of the NCMF. The rationael for placing this function at level 2 is because the function will be established by the overall controlling body, and will primarily assist with the prioritisation of national cybersecurity functions for implementation that happens at level 3. It will also inform the selection of national cybersecurity functions for implementation.

**Table 24: National strategic risk and threat assessment**

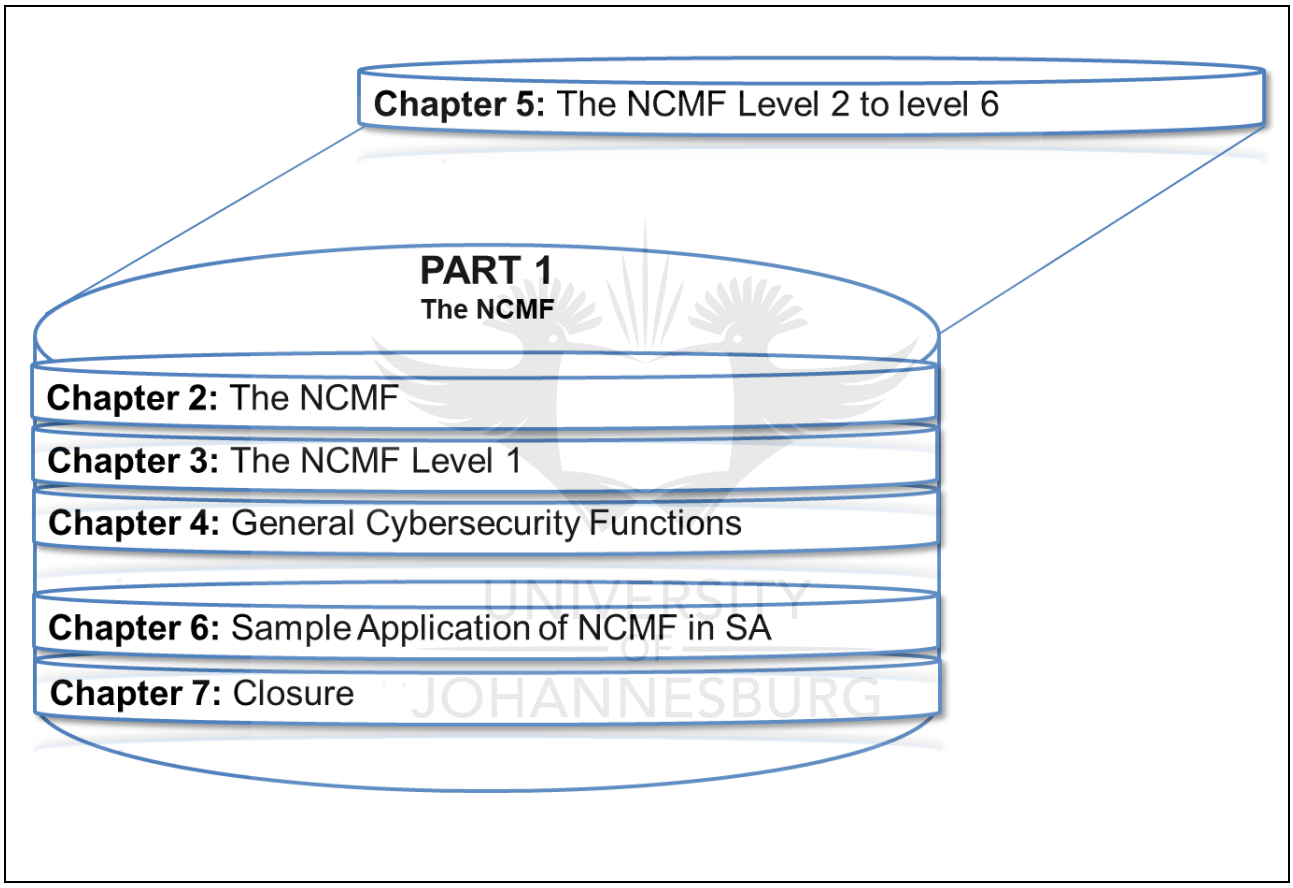
| Type | General cybersecurity function source | Source Document Location |
|---|---|---|
| **International normative** | The North Atlantic Treaty Organisation's (NATO) National Cyber Security Framework Manual (2011) [1] | 4.2.2 p113 |
| | The ITU National Cybersecurity Strategy Guide (2011) [100] | 16.1.2.1.2 p76 |
| | Cybersecurity Capability Maturity Model (C2M2) - Version 1.1 (2014) developed by the United States Department of Homeland Security [101] | 5.1 p19 |
| **National authoritative** | The National Cybersecurity Policy Framework (NCPF) [6], National Gazette No. 39475, 04 December 2015, Vol. 606 | 5.4.5 p82; 5.4.6 p82 |
| | The Cybercrimes and Cybersecurity Bill [34], Government Gazette No. 40487 of 9 December 2016 | 52(5)(e) p81; 52(5)(f) p81 |
| | The Protection of Critical Infrastructure Bill 2017 [90] | 7(a)(iii) p17; 9(2)(a)(ii) p20 |
| **International authoritative** | Irish National Cyber Security Strategy 2015-2017 (2015) [103] | 3.3 p10 |
| | Cyber Security Concept of the Slovak Republic (2015) [105] | Measure 5 p30 |



## 4.7 Conclusion

Chapter 4 started with a discussion on the aims we wanted to achieve with the identification of the general cybersecurity functions. Two aims were listed in Section 4.3. The first aim is to provide a pre-defined list of general and non-mandatory cybersecurity functions that countries can choose from for implementation. The second aim is for the predefined list of general cybersecurity functions to be used as a baseline against which the strategic applicability of the nation state's national cybersecurity functions may be measured against. Developing countries with their unique requirements and constraints, in the context of national cybersecurity were discussed in Section 4.4.

The thirteen general cybersecurity functions were introduced and discussed in detail. The selection of the *monitoring and evaluation*, and *incident handling* functions was motivated for use in the development of the E-CMIRC structure. The E-CMIRC structure is developed to illustrate the implementation part of the NCMF, and to provide a best practice guide for the development of national cybersecurity structures Part 2. The E-CMIRC structure will be developed by combining the services and technologies enabling these two selected functions. Following from here, Chapter 5 introduces and discusses level 2 to level 6 of the NCMF, ending with a presentation of the complete NCMF.



# Chapter 5: The National Cybersecurity Management Framework Level 2 to Level 6

## 5.1 Introduction

Chapter 3 introduced and presented level 1 of the NCMF. Level 1 lays the NCMF's foundation, and is used to discover a nation-state's national and international authoritative sources, and their cybersecurity functional prescripts. Chapter 5 serves to motivate and introduce level 2 to level 6 of the NCMF. We conclude this chapter with a consolidated view of the NCMF. The rest of the Chapter is structured as follows:

**Section 5.1** provides a motivation for the development of level 2 to level 5 of the NCMF.

**Section 5.2** introduces level 2. Level 2 motivates, and describes that a national risk-based approach should be followed to inform the selection, and drive the prioritisation of national cybersecurity functions for implementation. Level 2 also proposes the establishment of an overall controlling body.

**Section 5.3** introduces level 3. Level 3 serves as a placeholder to consolidate the selected and prioritised cybersecurity functions. This grouping allows for the identification of cybersecurity structures from where the functions will be offered from.

**Section 5.4** to **Section 5.9** introduces levels 4 to 6. These levels provide an implementation framework for the selected and prioritised national cybersecurity functions. The three options available to nation states during the application of level 3 of the NCMF (introduced in Section 5.5) are also discussed in more detail.

**Section 5.10** introduces the complete NCMF.

**Section 5.11** concludes this Chapter.

## 5.2 Motivation for NCMF Levels 2 to 6

We have described the desired characteristics of a National Cybersecurity Management Framework in Section 1.3 as being:

- Scalable,
- Flexible, and
- Agile.

Keeping the desired characteristics in mind, the decision was made in Section 2.9 to limit the NCMF to a maximum of six levels, without impacting on the efficiency and effectiveness of the framework. We impose this limitation to keep the framework simple, scalable, flexible and agile.

In Chapter 4, we have used level 1 of the NCMF to identify general cybersecurity functions, and actors. This activity resulted in a list of cybersecurity functions. Once the cybersecurity functions and actors are identified, the following management tasks remain:

- Selection of functions for implementation.
- Prioritisation of functions for implementation.
- Implementation of the selected and prioritised functions.

Responsibility for these tasks may be assigned to some of the actors that we have identified by using our stakeholder and actor identification template introduced in Section 3.5. We will now develop levels 2 to 6 of the NCMF to guide us with regard to these remaining tasks, and provide a high-level overview of levels 2 to 6 of the NCMF.

## 5.3 High-level overview of levels 2 to 6

It is our experience that the national cybersecurity management tasks of selecting, prioritising and implementing functions, will not happen unless explicit responsibility is assigned to national actors. This observation of ours is supported in the ITU's National Cybersecurity Strategy Guide [52]. We will now provide a high-level overview of the remaining NCMF levels, followed by a detailed description of each in the sections following.



### 5.3.1 Level 2 high-level introduction

The management tasks of selecting and prioritising the identified cybersecurity functions for implementation, lead to the requirement for a second level for the NCMF. It is our experience that these tasks will not happen unless explicit responsibility is assigned to national actors. This observation is supported in the ITU's National Cybersecurity Strategy Guide [52]. Level 2 prescribes the establishment of an overall controlling body. The overall controlling body is needed to initiate, drive and manage these tasks. Level 2 also prescribes the establishment of a national strategic risk and threat assessment process.

This process will inform and guide the selection, and prioritisation of functions for implementation. The motivation for placing an overall controlling body at level 2, is because this body must ensure that the NCMF is implemented from the top down as intended, and to drive the selection and prioritisation of cybersecurity

functions by means of the national strategic risk and threat assessment process. Responsibility for these tasks is explicit, and has to be assigned to actors by the overall controlling body.

### 5.3.2 Level 3 high-level introduction

After the application of level 2, we have a list of selected and prioritised national cybersecurity functions for implementation. We now need to identify the cybersecurity structures from where these functions will be offered. This allows us to identify the cybersecurity function's structure-specific functions, services and technologies. From these functions, we can then identify overlapping and similar functions services and technologies. In level 3, we consolidate the selected and prioritised national cybersecurity functions. This consolidation provides us with a logical grouping of cybersecurity functions, and we can use this to identify their structures and services.

### 5.3.3 Level 4 high-level introduction

The levels following level 2 of the NCMF (levels 3 to 6) are cybersecurity function, and structure specific. This means that the focus from level 2 onwards shifts from the *identification* of the mandatory or non-mandatory cybersecurity functions (level 1), and the *selection and prioritisation* of the functions (level 2), to the consolidation of functions (level 3), and *implementation* of the functions and their structures. Level 3 thus serves as the demarcation point where the implementation part of the NCMF starts. Level 3 provided us with a consolidated list of cybersecurity functions. In level 4, the structures supporting these functions are identified and consolidated.



These structures have their own functions and services. We will be using level 4 to determine the structure functions and services, and identify overlaps and similarities. For developing countries, these overlapping and similar functions and services may be combined, and offered from a new structure. Combining the functions and services of multiple structures, and offering them from a single structure, realise a cost and skills saving.

### 5.3.4 Level 5 high-level introduction

Since our framework is aimed at improving the national cybersecurity posture of nations, but with a focus on developing countries, the level 4 structures will be national structures, and will be subject to national acts and regulations. Level 5 is used to determine authoritative sources and their prescriptions applicable to the structures. These could be prescripts found in acts and regulations such as national health and safety, or physical security regulations if the structure is considered a national key point.

### 5.3.5 Level 6 high-level introduction

Level 6 addresses the operational elements of the national structure. These elements are all internal and examples are the structures policy, processes and procedures. Level 6 also addresses the technology needed to make the structure operational. The NCMF six levels, and the transition in focus from *identification, selection* and *prioritisation* to *implementation* is shown in Figure 24.

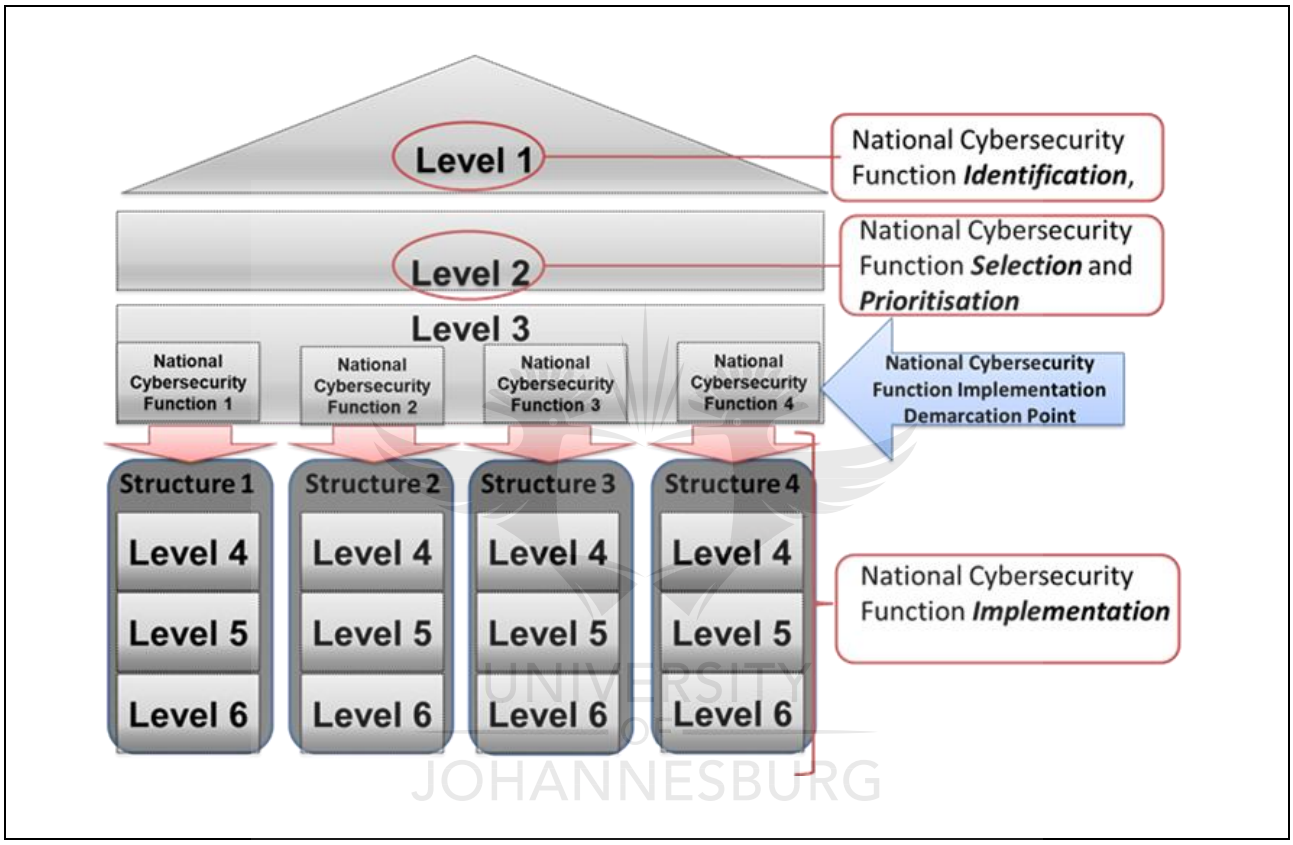



**Figure 24: Shift in Focus of NCMF Levels**

Figure 24 shows that the identification of cybersecurity functions happens at level 1 of the NCMF, and that the selection and prioritisation of those functions for implementation happens at level 2. The selected and prioritised functions are then consolidated, and their corresponding structures, with their services and capabilities are identified in level 3. The framework is structure specific from level 4 onwards. Level 4 to level 6 of the NCMF is used to determine structure specific elements needed (structure types, structure functions, services and technologies) to offer the national cybersecurity function.

Levels 2 to 6 is introduced and discussed in more detail in the following sections. We start our discussion with level 2, where the national, overall controlling body, as well as the strategic risk and threat assessment

function is described. During our discussion, we will use generic examples to illustrate the application of the NCMF levels, but we will also personalise the level discussions with our structures and templates, as well as South African actors, based on our experience.

## 5.4 NCMF Level 2 – National cybersecurity controlling body and strategic risk and threat assessment process

Level 2 describes the need for a national cybersecurity overall controlling body, and a N*ational strategic risk* and *threat assessment* function. In Chapter 4 we have identified the National Strategic Risk and Threat Assessment function as one of the thirteen general functions. This function was introduced in Table 11 in Chapter 4. A conscious decision was made to place the national strategic risk and threat assessment function at level 2 of the NCMF to support nation states during the selection and prioritisation of cybersecurity functions for implementation at national level.

The selection and prioritisation of national cybersecurity functions happen at level 2 of the NCMF, and through the application of the *national strategic risk* and *threat assessment* function. The use of the *national strategic risk* and *threat assessment function*, or a mechanism that will achieve the same outcome, is thus mandatory for nation states wishing to select and prioritise their mandatory, or non-mandatory cybersecurity functions for implementation. The outcome of the risk management process described in the national risk management guide, will, together with the dimensions, domains and mandates, largely dictate the selection and prioritisation of cybersecurity functions for implementation.



Although the national strategic risk and threat assessment function, or similar mechanism, is mandatory for nation-states wishing to select and prioritise their national cybersecurity functions, it is however not prescriptive in terms of standards, frameworks and approaches to be used. What matters though, is that this function is implemented to inform the selection and prioritisation tasks. Nation-states could make use of our national strategic risk and threat assessment guide (introduced in Appendix H with our recommended standards), or they can make use of their own frameworks and standards to guide them.

Our National Strategic Risk and Threat Assessment Guide (Appendix H) make a valuable contribution in that it provides a mechanism – with proven international standards – to conduct a national cybersecurity risk assessment. The outcome of such a risk assessment not only helps with the selection and prioritisation of cybersecurity functions, but it also helps nations understand the types of cyber risks they face and to develop strategies to mitigate those risks. The establishment and implementation of the national strategic risk and threat assessment function is the responsibility of the overall controlling body, and they must select the most suitable standard, framework or approach for their state, to execute cybersecurity risk management at national level. In developing countries, these overall controlling bodies still need to be established. The ITU in their

Global Cybersecurity Index (2017) [111], shows that out of forty-four African countries measured, only nine countries have an overall controlling body responsible for national cybersecurity.

This overall controlling body will have as its responsibility the implementation of the NCMF itself, as well as the implementation of the cybersecurity functions. Some of the activities that this national controlling body will execute, based on our experience, and supported by the ITU in their National Cybersecurity Strategy Guide [100] are to:

- Identify NCMF actors and stakeholders, and assigning responsibilities to them.
- Drive, steer and guide the *implementation of the NCMF*.
- Drive, steer and guide the *selection and prioritisation of national cybersecurity functions* for implementation. To assist with this task, the national strategic risk and threat assessment function is included in level 2 (refer to section 4.6.13).
- Drive, steer and guide the *implementation of selected and prioritised national cybersecurity functions*.
- *Identify existing national cybersecurity structures* from where the cybersecurity services enabling the selected national cybersecurity functions are offered..
- In the absence of existing structures, their responsibility would be to *envision and establish* new national cybersecurity structures.

In summary, the purpose of level 2 of the NCMF is to:

- Establish a national cybersecurity controlling body with the purpose of overseeing and controlling the application of the NCMF. It further oversees, steers and guide the identification, selection, prioritisation and implementation of cybersecurity functions through the implementation of the NCMF and its national strategic risk and threat assessment function.
- Establish a risk-based approach to do the prioritisation, and inform the selection of the cybersecurity functions for implementation through a national cybersecurity risk and threat assessment process,

Figure 25 presents the NCMF's second level, and illustrates that the overall controlling body, resides here. In South Africa, the SSA will typically be assigned the responsibility for the establishment of the overall controlling body, who, in turn, establishes the National Strategic Risk and Threat Assessment function. The national strategic risk and threat assessment function, also residing at level 2, is used to guide the cybersecurity function selection and prioritisation tasks.

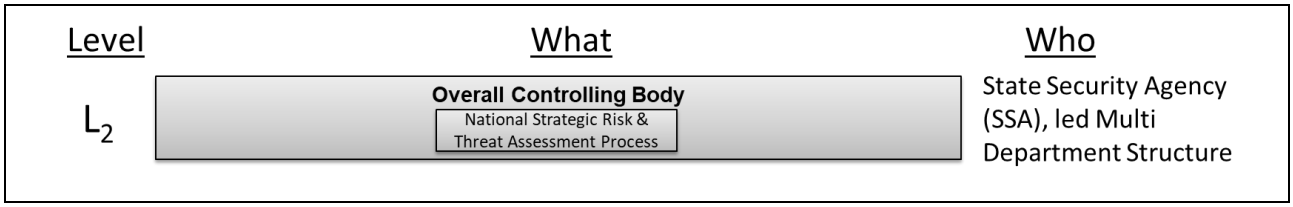



**Figure 25: NCMF Level 2**

Now that we have selected and prioritised cybersecurity functions for implementation at level 2, we will move to level 3 of the NCMF. Level 3 is used to consolidate the selected and prioritised national cybersecurity functions. This consolidation has as purpose the identification of their complementary structures, its associated functions, and technologies.

## 5.5 NCMF Level 3 – Consolidation

The identification of mandatory or non-mandatory national cybersecurity functions happens at level 1. The selection and prioritisation of national cybersecurity functions happen at level 2. The national cybersecurity functions that are selected and prioritised in level 2, are consolidated at level 3 of the NCMF. These functions give effect to national laws and treaty obligations, as well as national policies and strategies.

Once we have presented level 3, we will also introduce three scenarios describing how level 3 of the NCMF may be implemented. The three implementation scenarios are introduced in Section 5.6. The purpose of level 3 is:

- To provide a logical, structured placeholder to consolidate the selected and prioritised national cybersecurity functions. Consolidating the selected and prioritised cybersecurity functions is beneficial in that it drives the identification and the selection of existing structures, or the envisioning and development of new national cybersecurity structures that complement the selected and prioritised cybersecurity functions.
- Together with the defensive domain lifecycle phases introduced in Section 3.6.1, the cybersecurity functions selected and prioritised in level 2, could be prescriptive in the selection of national cybersecurity structures that are needed to offer them from.

Figure 26 shows the NCMF's third level. For the sake of completeness, and to illustrate the complete application of the NCMF in the context of identifying non-mandatory cybersecurity functions, we include the general functions that we have identified in Chapter 4.

It needs to be understood clearly that nation-states may identify many more or less mandatory or non-mandatory cybersecurity functions than the thirteen we have. Each nation's authoritative sources are unique. Nations may also select to use international normative sources different to the ones we have uses, and this will also influence the type and number of cybersecurity functions identified.

Twelve of the general cybersecurity functions are displayed in Figure 26. The thirteenth cybersecurity function, the national strategic risk and threat assessment function was displayed in Figure 25 as part of the NCMF level 2. The reason for this is, as we stated in Chapter 4, the *national strategic risk* and *threat assessment* function is one of the thirteen general cybersecurity functions that we identified in Chapter 4, and this function is placed at level 2 of the NCMF to support the selection and prioritisation of the cybersecurity functions for implementation.

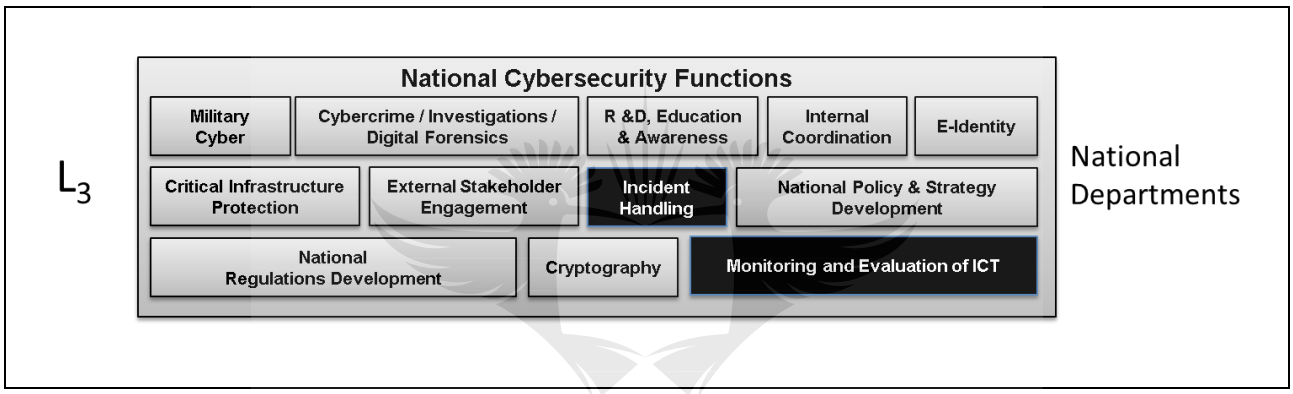



**Figure 26: NCMF level 3**

In terms of personalising the NCMF we have highlighted, in black, the two general cybersecurity functions that we have prioritised and selected for the development of our E-CMIRC in Part 2. These two general functions are the *incident handling*, and *monitoring and evaluation of ICT* functions. Each of the thirteen general cybersecurity functions must be handled as distinct areas of responsibility, and should be assigned to an appropriate government department for implementation.

One department may be assigned more than one function as its area of responsibility, such as the South African DOD being responsible for the military cyber function and the cryptography function. In most instances though, different government departments will be responsible for different structures, such as where the cybersecurity services are realising the *incident response* and *monitoring and evaluation of ict* function are offered from two different structures, and could fall under the auspices of two different government departments.

In Section 5.6, we will introduce three application scenarios for levels 1 to 3 of the NCMF. Our motivation for introducing and discussing the three implementation scenarios here, is that we had to introduce levels 1 to 3 first to allow the reader to get a solid understanding of the first three levels. This understanding is necessary since the implementation scenarios describe the three different ways in which nations can implement levels 1 to 3.

## 5.6 Implementation scenarios for NCMF levels 1 to 3

Now that we have discussed level 1 to level 3 of the NCMF, we would like to introduce and discuss our three application scenarios for the first three levels. We have stated in Section 5.2 that level 3 serves as the demarcation point where the implementation of cybersecurity functions start (implementation starts at level 4 and ends at level 6).

We have also introduced in Section 5.2 that level 1 identifies, level 2 selects and prioritises, and level 3 consolidates the selected and prioritised functions. We have identified three implementation scenarios for levels 1 to 3, and we will now introduce them.

We are introducing the three scenarios here, and before we start with our discussion on the levels following level 3. Levels 4, 5 and 6 focus on the implementation of the cybersecurity functions, and we will, thus, introduce our implementation scenarios before we start with the NCMF implementation levels. Our three implementation scenarios are:



- **Scenario 1**: Nation-states use our predetermined list of thirteen general cybersecurity functions but use their own mechanisms and criteria to select and prioritise them for implementation.
- **Scenario 2**: Nation-states use our predetermined list of thirteen general cybersecurity functions and use the NCMF National Strategic Risk and Threat Assessment function to assist with the selection and prioritisation of their national cybersecurity functions.
- **Scenario 3**: Nation-states use the NCMF to identify their own mandatory, and specific national cybersecurity functions. They then use the national strategic risk and threat assessment function to assist with the selection and prioritisation of their national cybersecurity functions.

We will now provide a more detailed discussion of the three scenarios.

- **Scenario 1**: In the first scenario, developed and developing countries select functions from our pre-determined list of thirteen general cybersecurity functions for implementation. The compilation of such

a list of general cybersecurity functions was described as one of our aims in Section 4.3. The implementation of one, or many of our thirteen general functions will have a positive impact on a country's national cybersecurity posture.

Levels 1 and 2 of the NCMF are thus not used at all, and nation-states start using the NCMF from levels 3 to 6. Nation states then use their own selection and prioritisation mechanisms, and criteria, to select one, or many of the general functions for implementation. Scenario 1 is depicted in Figure 27. It is shown in Figure 27 that nation-states only make use of the consolidated general cybersecurity functions, and use their own selection and prioritisation criteria and mechanisms.

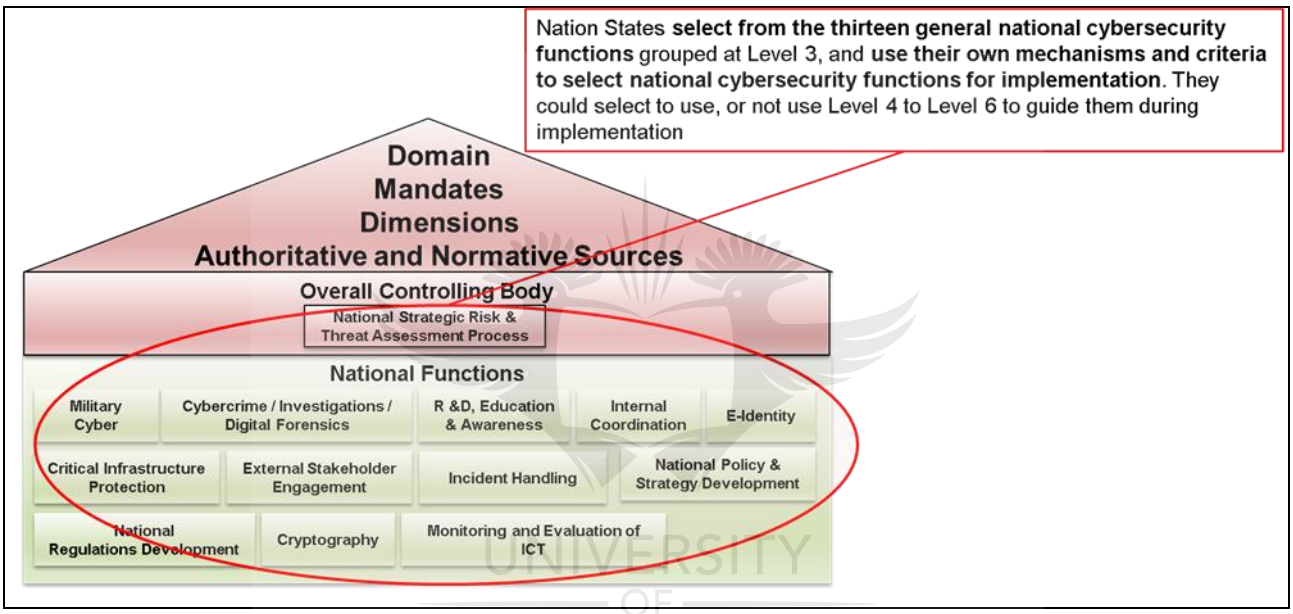



**Figure 27: NCMF application scenario 1**

Following scenario 1 does not make level 1 of the NCMF to a lesser importance. Level 1 of the NCMF is still applied to identify the cybersecurity functions, just not by the nation-state using the NCMF, but by us, as a third party. In scenario 1, the nation-state uses their own mechanisms and criteria to select and prioritise the general cybersecurity functions for implementation,

- **Scenario 2:** In the second scenario, nation-states use our pre-determined list of thirteen general cybersecurity functions, but use the NCMF national strategic risk and threat assessment function to assist with the selection and prioritisation of functions for implementation. This scenario is depicted in Figure 28. In scenario 2, only the list of consolidated, general cybersecurity functions, and the national strategic risk and threat assessment function from level 2 are used.

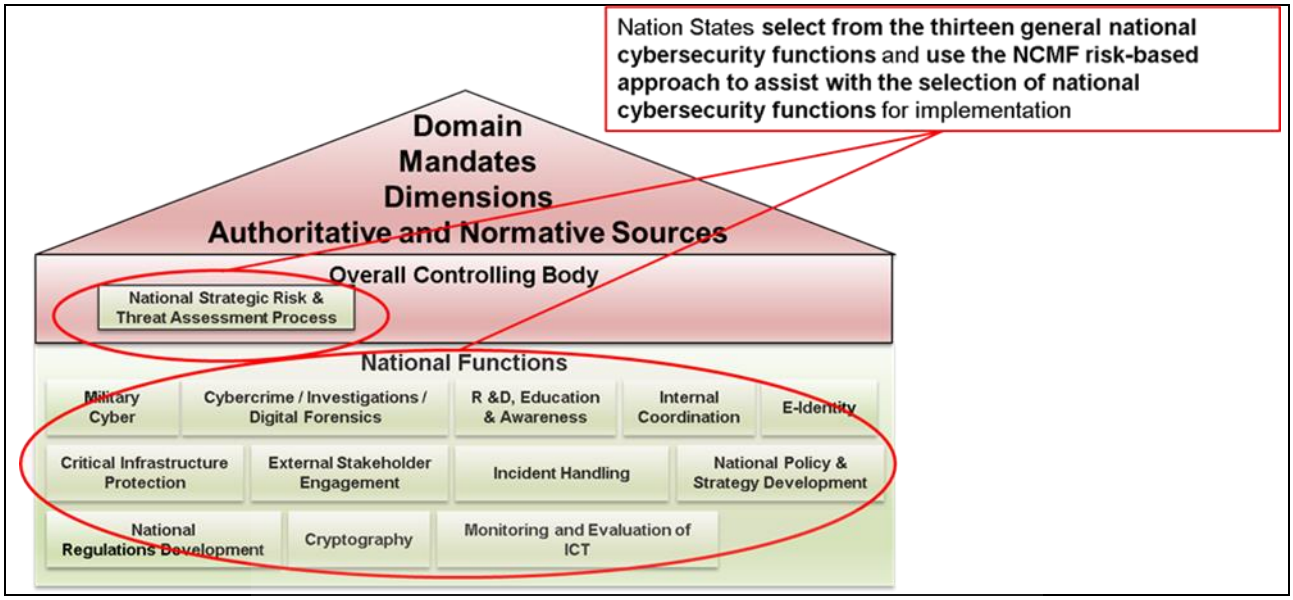



**Figure 28: NCMF application scenario 2**

- **Scenario 3**: In the third scenario, nation states use the NCMF to identify their own mandatory, and specific national cybersecurity functions. In this scenario, the NCMF is prescriptive in terms of the approach to be followed during the identification, selection and prioritisation of national cybersecurity functions.

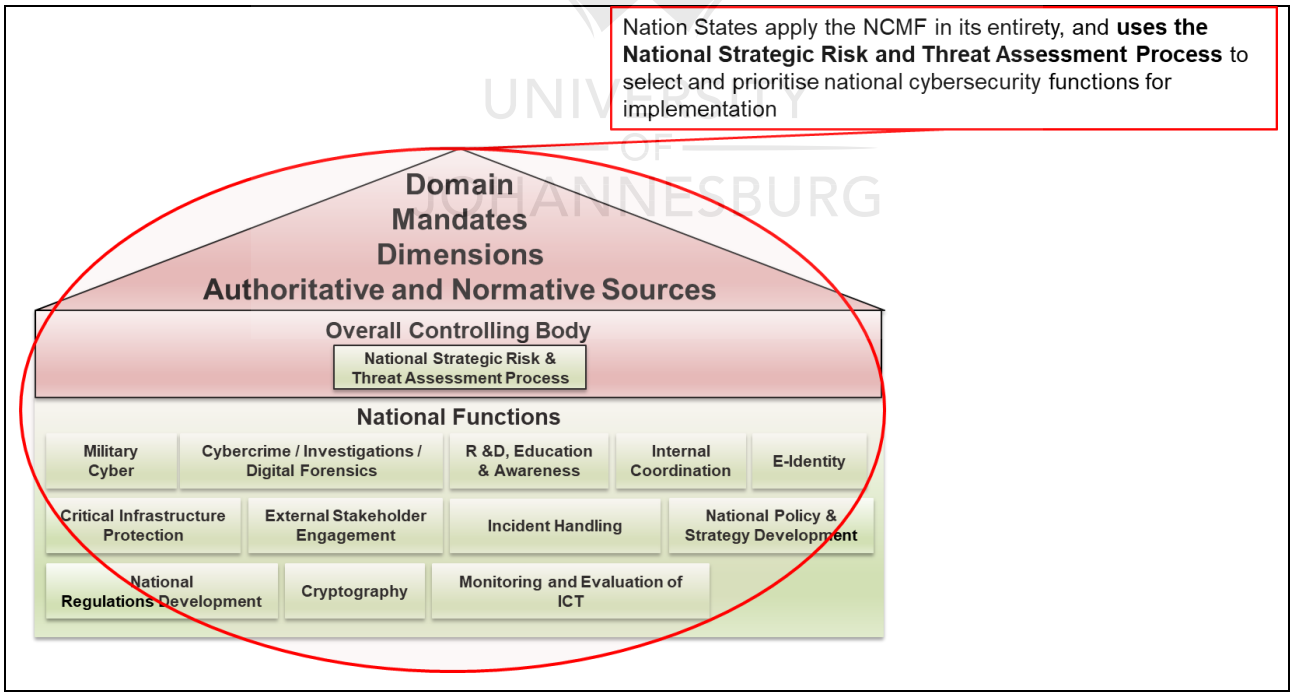



**Figure 29: NCMF application scenario 3**

This scenario is the only one where the use of our national strategic risk and threat assessment function is mandatory. The NCMF is applied in its entirety to assist nation-states with national cybersecurity functions management tasks. The discussion in Chapter 2 was done against the context of applying the NCMF in scenario 3.

In summation, developing countries could use any one of the three NCMF implementation scenarios. In the first scenario, the thirteen general cybersecurity functions could be used as a pre-determined list of functions from which they select one or many functions from for implementation. They use their own selection and prioritisation mechanism and criteria (they would thus follow their own approach to do the selection and prioritisation of cybersecurity functions for implementation).

They could also decide to use the second scenario where the pre-determined general cybersecurity functions are used, but the NCMF national strategic risk and threat assessment function is used to assist with the selection and prioritisation of cybersecurity functions. Using the third scenario, they would use the whole of the NCMF as described in Chapters 2 and 3.

In developing the E-CMIRC structure to illustrate the implementation part of the NCMF, we will follow the first scenario. This means that only the pre-determined list of thirteen general cybersecurity functions are considered. We have used, as a selection mechanism and criteria, our experience with the cybersecurity functions at national level, and based on this, selected two them, the *incident handling function,* and the *monitoring and evaluation function* to develop the E-CMIRC. It is thus not necessary for us to follow the risk-based approach prescribed by the NCMF, since we have already done our selection and prioritisation based on our experience with the two selected functions at national level. We will now in Section 5.7 continue or discussion of the NCMF level 4.



## 5.7 NCMF Level 4 – National structures

In Section 2.4, the terms “cybersecurity function,” “cybersecurity service” and “cybersecurity capabilities,” were introduced and defined. We explained that functions consist of services that are offered from national structures. We also described that cybersecurity services consist of capabilities that are made up of people, processes and technology.

The relationship between national cybersecurity functions, cybersecurity services, cybersecurity capabilities and structures were displayed in Figure 9. At level 4 of the NCMF, the national cybersecurity structures needed to deliver the cybersecurity functions that were consolidated at level 3, are defined. The purpose of level 4 of the NCMF is to:

- Identify existing national cybersecurity structures from where the national cybersecurity functions' are offered from. Where no national cybersecurity structures exist, new national cybersecurity structures need to be envisioned and established.
- To identify the actors responsible for the implementation of the national cybersecurity structure. These actors could be organs of state.

These national cybersecurity structures could be logical or physical in nature. An example of a logical national cybersecurity structure could be the E-Identity cybersecurity function introduced in Table 17. The E-Identity cybersecurity function consists of cybersecurity services and capabilities (people processes, and technology as defined in Section 4.6.6) and could be offered from a web portal.

The cybersecurity services realising the Incident Handling cybersecurity function (introduced in Table 18) are offered from structures such as CSIRTs [63]. The CSIRT national cybersecurity structures are typically physical, "brick and mortar" structures. These structures offer a facility from where the cybersecurity services realising the national cybersecurity functions are offered from. It offers a space to house people, and where incident handling related processes can be followed, tasks executed, or initiated, and where supportive cybersecurity technologies are deployed, housed and supported.

The E-CMIRC structure proposed in Part 2 to illustrate the application part of the NCMF, is a national cybersecurity structure that is housed in a centralised, physical facility. The E-CMIRC and all other national cybersecurity structures resides at Level 4 of the NCMF. A best practice guide to the establishment of national structures, such as our E-CMIRC structure, will be described in detail in Part 2. Figure 30 presents the NCMF's fourth level. Figure 30 shows that national cybersecurity structures could be structures such as CSIRTs and SOCs, and that our E-CMIRC is also a structure that resides here. We are including common structures, and personalise the level with our structure, the E-CMIRC, as explained in Section 5.2.

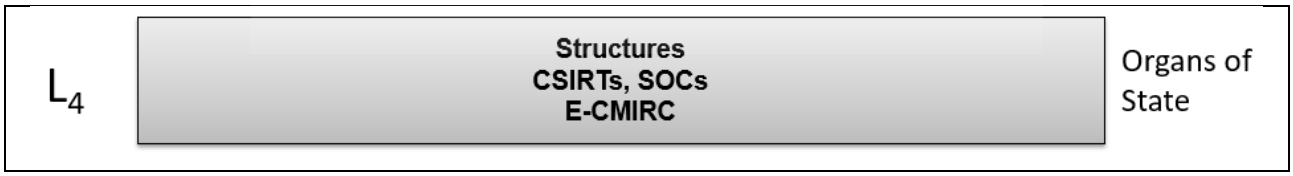



**Figure 30: NCMF Level 4**

## 5.8 NCMF Level 5 – Regulations for National Cybersecurity Structures

Level 5 specifies authoritative and normative sources needed in support of the structures with their associated services that they offer to facilitate cybersecurity functions. The purpose of level 5 of the NCMF is to identify

and, or, develop authoritative and normative documents applicable to the level 4 cybersecurity structures. The authoritative and normative documents are developed by the responsible actors that are identified during the application of level 1 of the NCMF. As mentioned in Section 3.9, and from a South African context, some of the organs of state actors could be SITA, DTPS, the DOD, and the SSA.

The level 5 authoritative and normative sources are specific to the structure, and could include physical security, or health and safety prescripts expressed in legislation or regulations. An example of regulatory bodies in a South African context is the Independent Communications Authority of South Africa (ICASA) [112] [113], and the National Energy Regulator of South Africa (NERSA) [114]. These regulatory bodies would exercise autonomous authority over, and regulate the activities of telecommunication providers (ICASA) and nuclear providers in South Africa (NERSA).

From a South African *national incident response* function perspective, the DTPS is responsible for developing regulatory requirements. The regulatory body is typically independent from the government [115]. Regulatory examples may include the security rating of the facility, its occupational health and safety requirements [116], and its physical security prescripts. The national cybersecurity structure's authoritative and normative prescripts and requirements are determined at level 4 of the NCMF. Figure 31 presents the NCMF's fifth level.

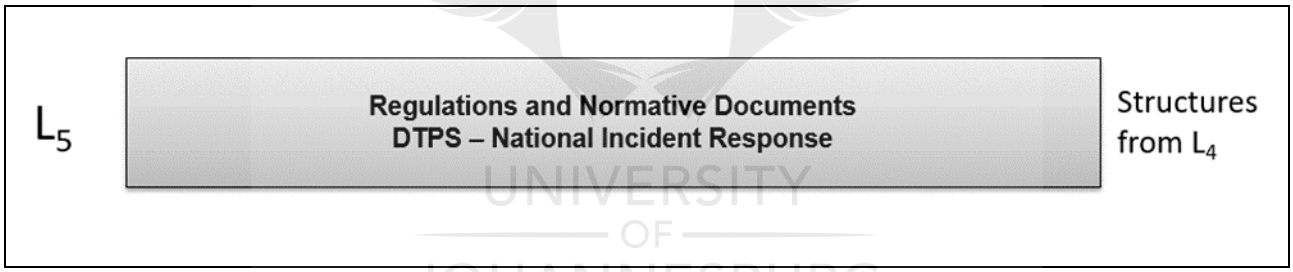





**Figure 31: NCMF Level 5**

## 5.9 NCMF Level 6 – Cybersecurity structure governance

From an operational governance perspective, the national cybersecurity structures need their own internal policies, processes and procedures. Level 6 describes the operational elements of the level 4 structures. These operational policies, processes and procedures are determined and developed in level 6 of the NCMF.

Examples of these elements could be the internal policies, processes, procedures and configuration standards describing and governing incident response for national incident response teams (CSIRT structure). Using the South African Cybersecurity Hub [82] as a case study, some examples of the operational documents are an incident handling policy, an incident management processes, back-up procedures, and password policies. In

the context of a SOC structure, an example of a policy could be the incident handling policy, and a process could be the monitoring process, or a shift handover process. These policies, processes procedures and standards enforce, and give effect to the regulations and normative documents as described in level 4.

Figure 32 presents the NCMF's sixth level. Figure 32 shows that structures such as the South African Cybersecurity Hub, and the newly envisioned E-CMIRC structure needs its own internal policies, processes and procedures. The purpose of level 6 of the NCMF is to develop and implement structure specific, internal, operational policies, processes and procedures. These policies, processes and procedures assists with the national structure's operational and governance requirements.

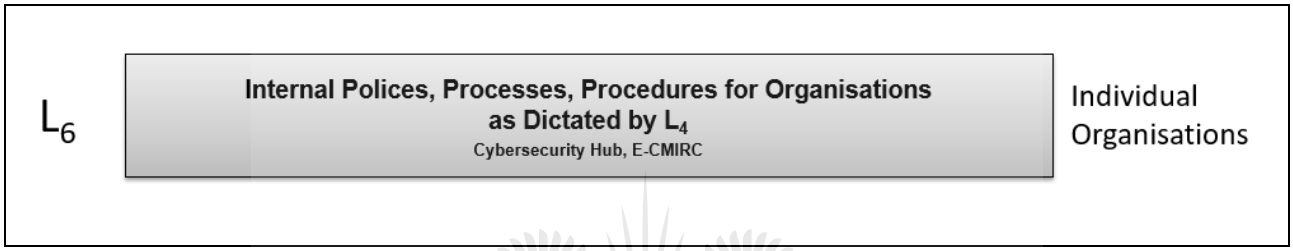



**Figure 32: Illustrative implementation of NCMF Level 6**

Now that we have concluded our discussion of the NCMF's level 1 in Chapter 3, and applied level 1 to identify thirteen of the most general cybersecurity functions in Chapter 4, and introduced and discussed levels 2 to 6 in this chapter, we will now, section 5.10 present the complete NCMF.



## 5.10 NCMF complete framework

Figure 33 presents the complete NCMF. It displays the overall structure of the NCMF with all the levels populated. Level 1 is used to identify national and international authoritative sources to determine nation state specific and mandatory cybersecurity functions. Level 1 can also be used to identify national and international normative sources to determine general cybersecurity functions.

We have used level 1 in Chapter 4 to identify national authoritative sources applicable to a developing country (South Africa), as well as international normative sources with its recommendations in terms of cybersecurity functions. Level 1 also identified the influencing elements. These are the cybersecurity dimensions, mandates and domains. Level 1 answers why cybersecurity functions are needed, and serve to assist in the identification and prioritisation of national cybersecurity functions. Level 2 concerns itself with the *selection and prioritisation* of national cybersecurity functions for implementation. Level 2 prescribes the need for a national overall controlling body, and also prescribes a risk-based approach. This risk-based approach is achieved by one of the thirteen cybersecurity functions, the national strategic risk and threat assessment function. We have

proposed a national cybersecurity risk management guide in Appendix H that nation states may use for their national risk management strategy. This risk-based approach further assists with the *selection and prioritisation* of cybersecurity functions for implementation. The overall national cybersecurity controlling body in level 2 should follow the PBRM organisational approach as a logical reference to ensure that all organisational aspects of the cybersecurity functions and its services are considered.

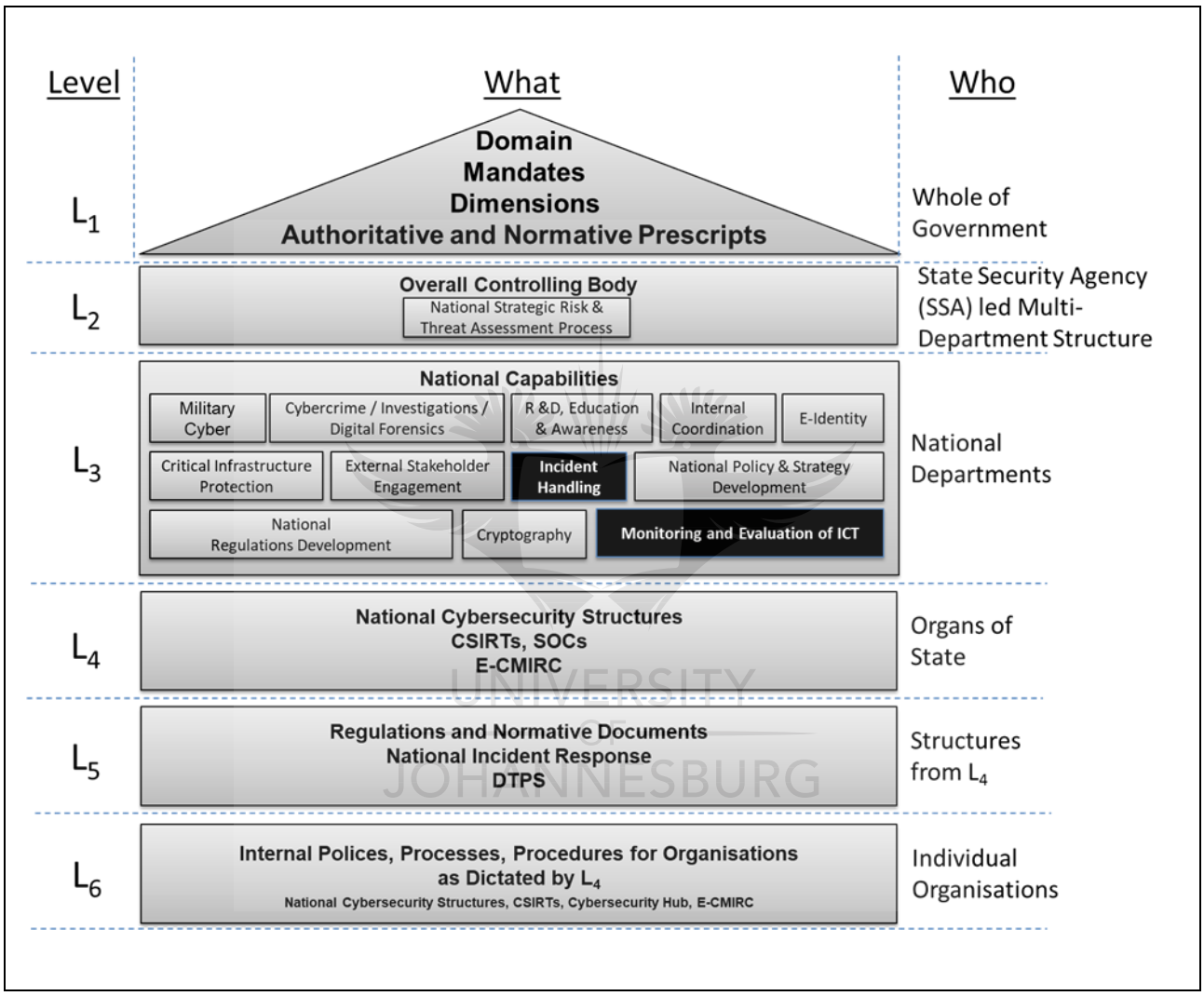



**Figure 33: The NCMF complete framework**

The national strategic risk and threat assessment function assists with the *selection and prioritisation* of cybersecurity functions. The selected and prioritised cybersecurity functions will be unique to each country. This is because their risks and threats in the cyberspace differ from each other. The cybersecurity functions of nation states will also differ since their authoritative and normative source prescripts and recommendations may differ.

Level 3 is used to consolidate the thirteen general cybersecurity functions. The general cybersecurity functions that we identified, were compared against international authoritative sources for completeness and relevancy. The two general functions (*incident handling* and *monitoring and evaluation* of ICT) that we have selected and motivated to illustrate the application of the NCMF's implementation part is shown in black. Level 3 serves as the demarcation point in the framework where the focus shifts from identification, selection and prioritisation, to the implementation of national cybersecurity functions.

Level 4 identifies national cybersecurity structures, as well as responsible organs of the state. These are actors, responsible for the implementation of the optimal national cybersecurity structures. The responsible actors will be selected from the list compiled from level 1 of the NCMF by using the stakeholder and actor identification template proposed in Table 8. These cybersecurity structures will house the people and technology that will enable the cybersecurity functions. The proposed E-CMIRC is a level 4 structure.

Level 5 describes the national cybersecurity structure's regulatory environment, and its authoritative and normative source prescripts are developed here. Level 6 describes the national cybersecurity structure's internal policies, processes and procedures. These internal policies, processes and procedures are operational in nature, and give effect to the national cybersecurity structure's authoritative and normative source prescripts that are developed in Level 5.

The NCMF is flexible in that it could be adapted for use in any of the dimensions, mandates and domains. Changes to authoritative and normative prescripts, as well as changes to the dimensions, mandate and domains of the NCMF will influence the identification, selection and prioritisation of the cybersecurity functions. The NCMF can also be applied to industry to improve the security posture of business entities [117].



## 5.11 Conclusion

Now that we have introduced the NCMF, and its six sequential levels, we will apply the NCMF in Chapter 6 in the context of a developing country, using South Africa as a reference country. The levels are populated using South African authoritative and normative sources, overall controlling bodies, national cybersecurity functions and structures.

In this Chapter, the NCMF level 2 to level 6 was introduced. The NCMF consists of six levels, starting with level 1 and ending with level 6. The purpose of NCMF level 1 to level 2 is to guide, steer and inform the national cybersecurity management tasks of *identification, selection and prioritisation* of national cybersecurity functions. The purpose of the NCMF Level 3 to Level 6 is to guide, steer and inform the *implementation* of

national cybersecurity functions. The NCMF follows a top-down hierarchical approach, and it is flexible enough for use by nation states, and at organisational level.

Section 5.2 provided a motivation for NCMF level 2 to level 6. It confirmed the desired characteristics of a NCMF as being scalability, flexibility, and agility. These characteristics place a limit on the number of framework levels. The identification of actors and their responsibilities were discussed. Some of their responsibilities are to implement the NCMF, and to implement the national cybersecurity functions.

Section 5.3 provided a high-level overview of levels 2 to 6.

Section 5.4 introduced level 2 of the NCMF. Level 2 prescribes the establishment of an overall national controlling body and a risk-based approach to do the selection and prioritisation of national cybersecurity functions for implementation. It was illustrated how the list of cybersecurity functions is determined from national and international authoritative and normative sources, and that these sources could prescribe, or recommend nation state specific and mandatory, or general cybersecurity functions. The outcome is that level 3 is populated with the selected and prioritised cybersecurity functions.

Section 5.6 introduced level 3 of the NCMF. Level 3 serves as a placeholder to consolidate the selected and prioritised cybersecurity functions. The selected and prioritised cybersecurity functions are used to identify national cybersecurity structures, and their services. The three scenarios that nation-states may consider when using level 1 to level 3 of the NCMF were also described.



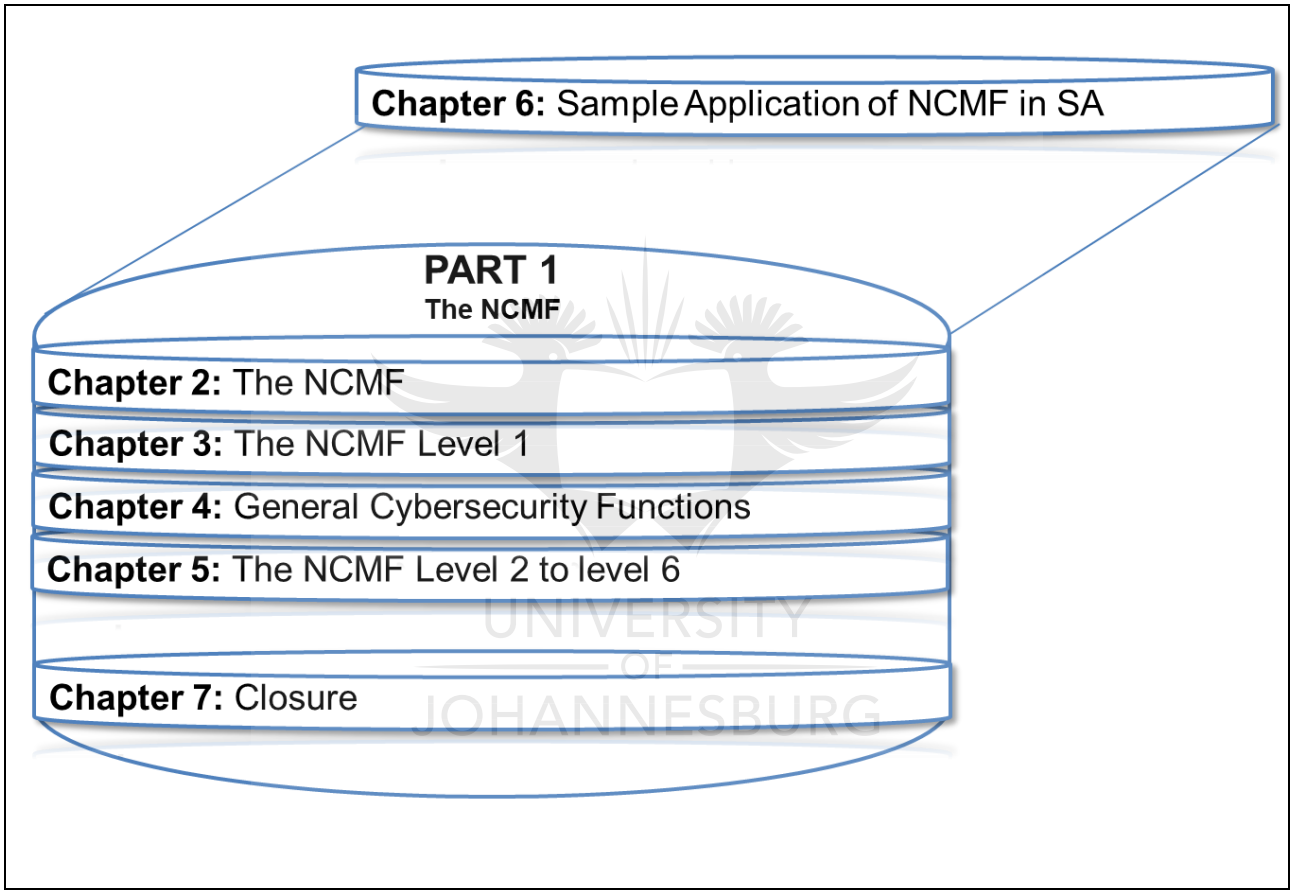
Section 5.7 introduced level 4 of the NCMF. This level identifies and houses the national cybersecurity structures needed to offer the selected and prioritised cybersecurity functions from, as well as its actors.

Section 5.8 introduced level 5 which considers regulations, authoritative and normative prescripts applicable to the national cybersecurity structures.

Section 5.9 introduced level 6. Level 6 considers operational elements of the national cybersecurity structure, such as structure specific policies, processes and procedures.

Section 5.10 introduced the complete NCMF with its six levels.

In Chapter 6 we will use apply the NCMF in the context of South Africa. We do this to illustrate the application of the NCMF at a national level, for a developing country. The application of the NCMF and the population of the framework is done based on our work experience, executing cybersecurity projects at national level in South Africa.



# Chapter 6: Sample Application of NCMF in South Africa

## 6.1 Introduction

The NCMF was introduced in Section 2.9, and level 1 was discussed in detail in Chapter 3, while level 2 to level 6 were discussed in detail in Chapter 5. The NCMF consists of six hierarchical levels starting at level 1. The sample application of the NCMF is done in the South African context, and uses the *incident handling* and *monitoring and evaluation* general cybersecurity functions that we identified in Chapter 4, and consolidated in level 3. The services from these two functions are combined, and offered from a new level 4 national structure. The envisioned application of each level is presented in the text below.

**Section 6.2** to **Section 6.7** illustrate the application of the NCMF levels in context of South Africa as a reference developing country.

**Section 6.8** concludes this chapter.

## 6.2 NCMF Level 1 – Identify South African authoritative and normative sources

The NCMF level 1 was introduced in Chapter 3. As stated in Section 3.3, the purpose of level 1 of the NCMF is to identify national and international authoritative and normative sources, and to identify mandatory national cybersecurity functions, or non-mandatory cybersecurity functions from those sources. Level 1 is further used to identify actors by considering the NCMF dimensions.



Some of the South African authoritative and normative sources found during our research, are the NCPF [6], South African Cybercrimes and Cybersecurity Bill [34], Protection of Critical Infrastructure Bill [90], The Protection of Personal Information Act 4 of 2013 [39], Electronic Communications and Transactions Act of 2002 [118], and government requirements expressed in the Department of Public Service and Administration (DPSA) Public Service Corporate Governance of Information and Communication Technology Policy framework which requires that COBIT 5 be adopted by public sector organisations [119].

Following the identification of these national and international authoritative and normative sources, the mandatory cybersecurity function prescripts expressed in them are identified. As an example, and from a South African national policy perspective, the NCPF [6] prescribes that cybersecurity in South Africa be improved. [34]. The NCPF then further prescribes the establishment of a national Incident Handling function [6] as one means of achieving this. The establishment of a national incident handling function is also prescribed by the South African Cybercrimes and Cybersecurity Bill [34].

The South African Cybercrimes and Cybersecurity Bill [34] however goes into more detail, in that it prescribes the establishment of additional structures that need to be established to offer functions such as the ECS-CSIRT (the incident handling function for government), the Cybersecurity Hub (the critical information infrastructure protection (CIIP) function), the cyber command (the military cyber function) and the Cyber Crimes Center (the cybercrimes / investigations / digital forensics function). The South African Cybercrimes and Cybersecurity Bill also assigns responsibilities to government departments and organs of state for the establishment of these national cybersecurity structures. The functions, their structures and responsible organs of state is displayed in Table 25.

**Table 25: South African cybersecurity functions, structures and responsibilities**

| National Cybersecurity Function | Structure | Responsibility |
|---|---|---|
| Incident handling | ECS-CSIRT | SSA |
| Critical information infrastructure protection | Cybersecurity Hub | DTPS |
| Military cyber /cyber warfare | Cyber Command | DOD |
| Cybercrimes / investigations / digital forensics | Cyber Crimes Centre | SAPS |

The cybersecurity dimensions, mandates and domains in which the NCMF operate, inform and augment the identification, selection and prioritisation of cybersecurity functions. The NCMF government, national and international dimensions assist with the identification of actors. Responsibility for the implementation of the NCMF, as well as the implementation of cybersecurity functions, could be assigned to the actors identified. The dimensions were introduced and discussed in Section 3.5.



The NCMF can further operate in either the offensive, or defensive domain. The defensive domain lifecycle phases can assist with the selection and prioritisation of cybersecurity functions, in that different cybersecurity functions and structures are needed during each of the lifecycle phases of the defensive domain. The domains were introduced and discussed in Section 3.6.

The NCMF mandate also informs the selection and prioritisation of cybersecurity functions. As an example, the mandate of the NCMF during time of war will be to identify and implement cybersecurity functions in support of military cyber, or cyber intelligence and counter-intelligence. Rising national cybercrime levels could shift the mandate of the NCMF to the identification and implementation of national cybersecurity functions in support of counter cybercrime efforts. These are all possible mandates for the NCMF, and will influence the selection and prioritisation of national cybersecurity functions. The mandates were introduced and discussed in section 3.8.

To illustrate the application of the NCMF, in the context of South Africa as a developing country, the defensive domain is selected as the domain of operation, with the critical information infrastructure protection (CIIP) and national crisis management as its mandates. The selection of the defensive domain and critical information

infrastructure protection (CIIP) and national crisis management mandate were motivated in sections 3.7 and 3.9.

The cybersecurity *incident handling* and *monitoring and evaluation* of ICT national cybersecurity functions reside in the defensive domain, and deliver on the critical information infrastructure protection (CIIP) and the national crisis management mandate. Their complementary cybersecurity structures are CSIRTs and SOCs as introduced in Appendix A.

## 6.3 NCMF Level 2 – Establish a South African national cybersecurity controlling body

This level describes an overall controlling body that is responsible for implementing the NCMF, and also the national cybersecurity functions as expressed by the NCPF [6] and the South African Cybercrimes and Cybersecurity Bill [34]. Examples of such controlling bodies in the South African context, are the Cyber Response Committee (CRC) [120] and the National Cybersecurity Advisory Council (NCAC) [121], as mandated by the NCPF [6]. The role of these controlling bodies is to oversee, steer and guide the planning, as well as the building, running and monitoring of the national cybersecurity structures from where the national cybersecurity functions are offered..

In South Africa, the SSA leads this multi-departmental approach. The function of the overall national cybersecurity controlling body is to ensure that the national cybersecurity structures needed for the national functions, are planned, built, ran and monitored. The appointed CRC, chaired by the SSA, will oversee and steer the implementation of national cybersecurity functions in South Africa. As an advisory body, the National Cybersecurity Advisory Council (NCAC) [122] may also influence the national cybersecurity agenda.

The national strategic risk and threat assessment function resides at level 2, and promotes the selection and prioritisation of national cybersecurity functions through a risk-based approach. For example, the national strategic risk and threat assessment function's processes identify the lack of national incident response and co-ordination at national level as a high risk, and flags the *incident handling* function for selection as a national cybersecurity function, and prioritises the establishment of a national *incident handling* function.

The national strategic risk and threat assessment function could be based on international standards such as ISO/IEC 27005:2011 – information security risk management [123], or any nation state-specific risk and threat assessment methodology. To provide nation states with a starting point, we have proposed a National Cybersecurity Risk and Threat Management Guide in Appendix H.

Now that a national cybersecurity controlling body has been established, as well as a mechanism for steering the selection and prioritisation of national cybersecurity functions for implementation, the NCMF's level 3 captures and consolidates the identified, selected and prioritised national cybersecurity functions.

## 6.4 NCMF Level 3 – Consolidate national cybersecurity functions

The output from level 1 and level 2 – the selected and prioritised national cybersecurity functions, are consolidated at level 3. As stated in section 5.5, the cybersecurity functions can be nation-state specific and mandatory, or general. Level 3 is flexible and will change as and when a nation state's cybersecurity posture changes. Structures at level 4 are selected based on the national cybersecurity functions consolidated in level 3.

The levels following level 3 of the NCMF (levels 4 to 6), are cybersecurity structure specific, as described in section 5.2 and displayed in Figure 24. To illustrate the sample application of the NCMF in a South African context, the *incident handling*, and *monitoring and evaluation of ICT* general cybersecurity functions are selected. These two national functions' structures, their functions, complementary services and technologies are identified in Appendices B and C. Now that the cybersecurity functions have been identified, selected and prioritised, and consolidated in level 3, the optimal cybersecurity structure need to be identified, from where the national cybersecurity function, and its cybersecurity services will be offered from. Level 4 of the NCMF identifies the optimal national cybersecurity structures.

## 6.5 NCMF Level 4 – Structures realising the cybersecurity functions

The national cybersecurity structures could be centralised, or decentralised. National-CSIRTs can be considered as an example of a decentralised structure. These structures typically consist of a top-level structure, the national-CSIRT, with distributed sector-CSIRTs. In South Africa, the Cybersecurity Hub serves as the national-CSIRT, with the South African Banking Risk Information Centre serving as a banking sector-CSIRT [124].

This type of structure is typically decentralised, with sector-CSIRTs feeding, and reporting into, the national-CSIRT [125], [126]. The national cybersecurity structures may also be a structure that is physical, or logical in nature, or a combination of the two. An example of a national cybersecurity function offered from both a physical and a logical structure, is the South African national cryptography cybersecurity function, which is offered by the South African Communications Security Agency (SACSA) [110]. The responsibility of SACSA is to consider and develop national cryptography policies, and public key infrastructures (PKI) [127]. It is our experience that this function is offered from a single, centralised physical structure (building) housed in South Africa, using a logical structure (technology framework and processes) to develop national policies and solutions.

From a South African context, the National Cybersecurity Policy Framework (NCPF) [6] and the Cybercrimes and Cybersecurity Bill [34] prescribe the establishment of four national cybersecurity structures. In South Africa, the national CSIRT or Cybersecurity Hub [82], as mandated by the NCPF [6], falls under the auspices of the Department of Telecommunications and Postal Services (DTPS), and it realises the national *incident handling* cybersecurity function. None of the South African authoritative sources, however, prescribe a *monitoring and evaluation* function.

Most international normative sources, however, have strong references to such a function such as ISO/IEC 27001:2013 [128], COBIT 5 [129] and NIST SP 800-39 [9] to name a few. The services and technologies that enable and realise the *monitoring and evaluation* function, is offered from structures such as SOCs [19]. In South Africa, the responsibility for the establishment of these structures may fall under the auspices of the State Information Technology Agency (SITA) [3].

Some additional national cybersecurity structures prescribed by the NCPF are the Cyber Command which is a Department of Defence (DOD) responsibility [34], the Cybercrimes Centre – a South African Police Service (SAPS) responsibility [34] and the government-CSIRT known as the Electronic Communications Security CSIRT (ECS-CSIRT) which is a State Security Agency (SSA) responsibility [34].

Where it concerns *Incident Handling* at national level in South Africa, the DTPS is responsible to build a structure called the Cybersecurity Hub that serves as the South African national CSIRT. One of the mandates of the Cybersecurity Hub is to promote the building of additional structures called Sector-CSIRTs [34]. The Cybersecurity Hub is the South African national cybersecurity structure that offers the services that enables and realises the national *Incident Handling* function.



Once the actors responsible for the implementation of a national cybersecurity function, as well as its optimal structure are identified, regulations and prescripts related to the national cybersecurity function and its structure need to be determined, and developed if needed. These regulations and prescripts, expressed in authoritative and normative sources, influences the operations and services that are offered from the national structure, as well as its governance.

## 6.6 NCMF Level 5 – Regulations for national cybersecurity structures

From a South African perspective, and using the *incident handling* cybersecurity function as an example, it is prescribed by the NCPF that the DTPS must be held responsible for the national *incident handling* function, with the national Cybersecurity Hub identified as the optimal national cybersecurity structure [33]. The DTPS is responsible for developing authoritative and normative sources applicable to the South African *incident handling* function at national level. These sources may contain regulatory requirements and standards.

## 6.7 NCMF Level 6 – Cybersecurity structure governance

Level 6 of the NCMF describes the national cybersecurity structure's governance requirements. From a South African perspective, these would be the Cybersecurity Hub internal policies, processes, procedures and standards applicable to the structure itself, and the daily operations of the Cybersecurity Hub.

## 6.8 NCMF consolidated application

The application of the NCMF in the context of South Africa as a developing country is shown in Table 26.

**Table 26: NCMF Applied to South Africa**

| NCMF Level | South Africa |
|---|---|
| **National cybersecurity identification function** | |
| **NCMF Level 1 (L1)** | **Domain:** Defensive domain.<br>**Mandate:** Critical information infrastructure protection (CIIP) and National crisis management.<br>**Dimension:** Government (SSA, DOD, DTPS, SITA) National (SABRIC) international (FIRST).<br>**National authoritative sources:** NCPF, South African Cybercrimes and Cybersecurity Bill, Protection of Critical Infrastructure Bill, The Protection of Personal Information Act 4 of 2013, Electronic Communications and Transactions Act of 2002.<br>**National normative:** COBIT 5.<br>**Mandatory national cybersecurity functions**: Incident handling and monitoring and evaluation of national ICT as prescribed by NCPF and applicable to the selected domain and mandates. |
| **National cybersecurity selection and prioritisation function** | |
| **NCMF level 2 (L2)** | **Overall controlling body:** National Cybersecurity Advisory Council.<br>**National strategic risk and threat assessment process:** Using ISO/IEC 27005:2011. |
| **National cybersecurity function implementation** | |
| **NCMF level 3 (L3)** | After application of the national strategic risk and threat assessment process, a selection and prioritisation of the identified national cybersecurity functions takes place. In our example, the national *incident handling* and *monitoring and evaluation of national ICT* functions are selected and prioritised for implementation. |
| **NCMF level 4 (L4)** | Structures identified from where the selected and prioritised national cybersecurity functions are offered from as determined by considering the Defensive Domains lifecycle phases. The structures at national level is a CSIRT, and at organisational level, a SOC. For illustration, a CSIRT is selected. |

| | |
|---|---|
| **NCMF level 5 (L5)** | SAPS Act 68 of 1995 [130] provides prescripts in terms of physical security, and the Occupational Health and Safety Act (No. 85 of 1993 ) [43] provides prescripts in terms of occupational health and safety. |
| **NCMF level 6 (L6)** | **Policy:** National incident management policy, acceptable use policy, mail policy, for example.<br>**Process:** Incident management process, escalation process, back-up process<br>**Procedure:** Symantec netbackup procedure. |

Table 26. Shows the dimensions, mandates and domains we have selected to illustrate the application of the NCMF, and it also shows the South African national authoritative, as well as national normative sources. We further show that we have selected the *incident handling* and *monitoring and evaluation of* cybersecurity functions. We also show that the overall controlling body and the national strategic risk and threat assessment process resides at level 2. We contextualised the overall controlling body for South Africa.

Levels 3 to 6 describe the implementation of national cybersecurity functions and their structures. Level 3 is used to consolidate the selected and prioritised functions and level 4 identifies the cybersecurity function's complementary structures. Levels 5 and 6 are structure-specific, and identifies authoritative and normative prescripts related to the structure, as well as operational and governance requirements for the structure.

Now that the NCMF is presented, and its application illustrated in the context of South Africa as a reference developing country, a mechanism is proposed for its implementation by nation states. Appendix I proposes that the implementation of the NCMF be made a government responsibility. The responsibility for the implementation of the NCMF may be delegated to the national overall controlling body.

The NCMF should operate at the strategic level of government operations. It is important to have an implementation plan for the NCMF since, without such a plan, the NCMF will remain a framework on paper only. Following an implementation best practice will assist with defining an implementation strategy, align actors and stakeholders, and assist with assigning responsibilities in terms of implementing the NCMF. In Appendix I we provide an NCMF best practice implementation guide.

## 6.9 Conclusion

In this chapter, we have illustrated the working of the NCMF by applying it to South Africa as a reference developing country. Section 6.2 to Section 6.6 covered the six levels of the NCMF, and we presented a sample application of the NCMF's six levels in the context of South Africa as a developing country.

Chapter 6 concludes our discussion of the NCMF. We have introduced the NCMF and illustrated its application in context of South Africa as a developing country as listed below:

- In Chapter 3 we developed level 1 of the NCMF.
- We then used the NCMF level 1 in Chapter 4 to identify thirteen of the most general cybersecurity functions.
- Chapter 5 was used to develop levels 2 to 6 of the NCMF.
- In Chapter 6 we presented a sample application of the NCMF in the context of South Africa as a developing country.

The reader should now have a good understanding of our intended application and usage of the NCMF. The key aspects of the NCMF we would like to highlight are:

- The NCMF consists of 6 levels.
- Levels 1 and 2 of the NCMF identify, select and prioritise national cybersecurity functions through the identification of national and international authoritative and normative sources. It also considers input from influencing elements such as dimensions, domains and mandates. The identified, selected and prioritised cybersecurity functions are consolidated in level 3.
- Levels 4 to 6 of The NCMF describe how to implement national cybersecurity functions.
- Cybersecurity functions consist of services that are made up of capabilities. Services and capabilities are made up of people, processes and technologies, and are offered from national cybersecurity structures.
- Nation states using the NCMF should follow a phased approach, and only implement one or two functions at the most, at a time.
- The general cybersecurity functions we have identified may be analysed and compared with the functions and services offered by existing national and commercial cybersecurity structures to identify overlapping or similar services, technologies and skills needed to enable them.
- Nation states may realise costs and skills saving by combining and then offering the services and technologies from two or more functions from a single structure.

Chapter 6 concludes Part 1. In Part 1, we developed the NCMF. We have also identified thirteen general cybersecurity functions and explained in Chapter 1 that national cybersecurity functions are offered from national cybersecurity structures. In Part 2, we propose a best practice guide that nation-states can use when building, running and monitoring national cybersecurity functions. Part 2 is meant to illustrate the application of the NCMF which we developed in Part 1. It is not necessary for the reader to read Part 2 in as much detail as Part 1, since Part 2 is seen as an operational guide, and it is a secondary deliverable.

## 6.10 Summative model for part 2

We have stated in Section 1.1 that we have selected and motivated for the use of the PBRM organisational approach for the development of our NCMF. The NCMF assisted us to identify general cybersecurity functions, and satisfied the plan function of the PBRM organisational approach. Throughout this thesis we have made mention of functions, services and capabilities. We have also discussed structures. Each of the cybersecurity

functions have services and capabilities associated with them, and these serve to enable them. These national cybersecurity functions are then offered from cybersecurity structures.

Where the NCMF addresses the plan function of the PBRM organisational model, our E-CMIRC's descriptive models will address the build, run and monitor functions of the PBRM organisational approach. To assist us in envisioning a new structure, we will first look at existing structures from where the *incident handling*, and *monitoring and evaluation* functions may be offered from. We have identified two existing structures – SOCs and CSIRTs that offer the *incident handling*, and *monitoring and evaluation* functions respectively.

Part 2, provides an example of how a structure such as the E-CMIRC may be developed. We are developing the E-CMIRC structure to illustrate the application of the NCMF. We have selected and motivated for the use of the *monitoring and evaluation*, and the *incident handling* cybersecurity functions to illustrate the implementation part of our NCMF. Using these two cybersecurity functions as a reference, we will identify their complementary cybersecurity structures. The *monitoring and evaluation* function's complementary structure is the SOC, and the *incident handling's* complementary structure is the CSIRT.

The SOC and the CSIRT have their own functions and services. It needs to be mentioned here again that a function consists of a service, and that a service is made up of a capability that, in turn, are made up of people, processes and technologies. In Part 2 in Appendices B and C, we will identify the SOC and CSIRT functions and services. Our primary intention is to identify the SOC and CSIRT functions with overlapping services and capabilities.



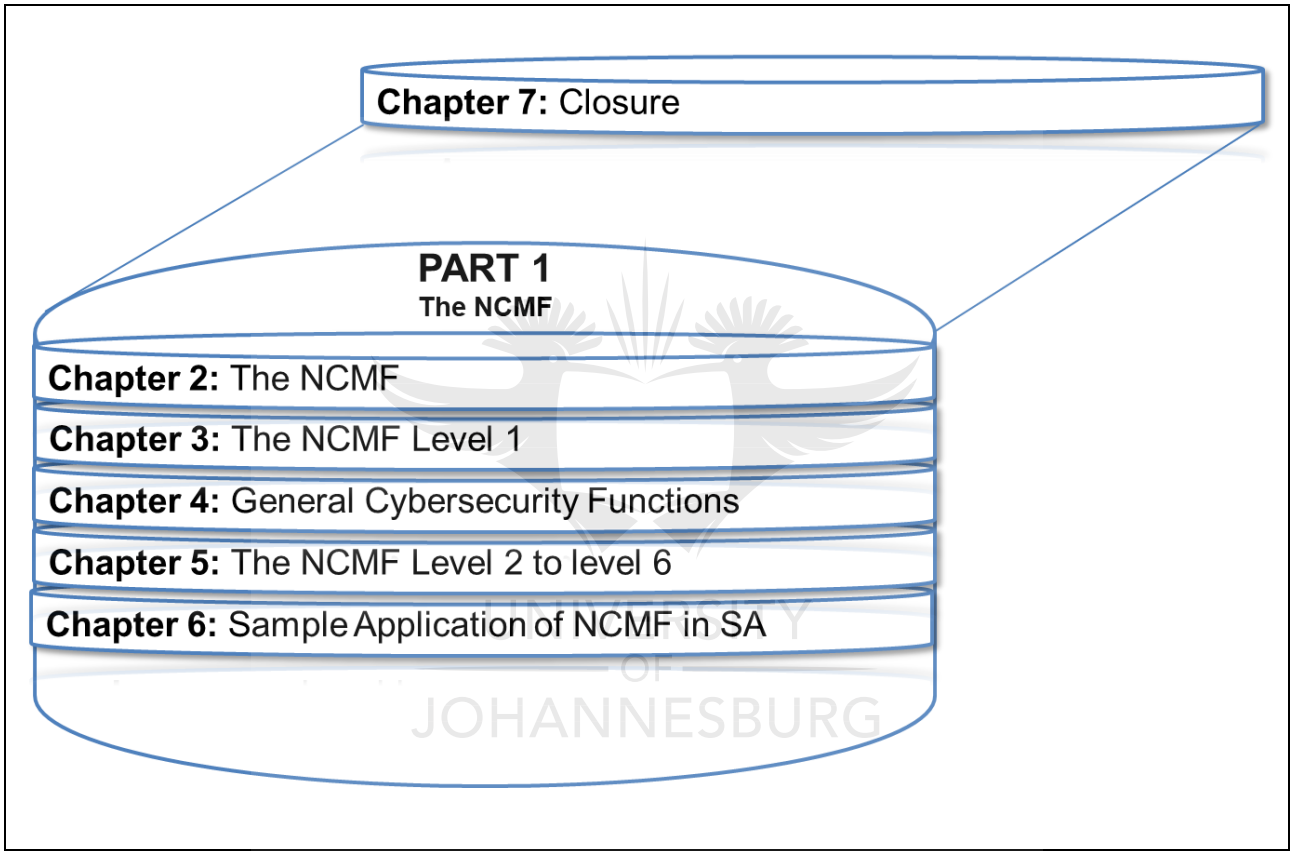
Our E-CMIRC structure will offer a combination of the SOC and CSIRT functions and services. By combining the functions and services with its supporting technologies, developing countries can realise a cost benefit. This may be achieved by offering them from a single structure, using a common technology and processes. It further results in skills saving, in that a lesser number of technologies need to be supported, managed and maintained.

Appendix A introduces the SOC, and CSIRT structures where the *monitor and evaluation* function, and the *incident handling* function is offered from. SOCs are sometimes referred to as cyber intelligence centres (CIC) [131]. The discussion of these two structures will be general in nature, and an initial understanding of these two structures and their service delivery models will assist the reader in understanding the detailed discussion of their functions and services following in Appendices B and C. Part 2 is structured as follows:

- Appendix A, is used to introduce SOCs and CSIRTs, and provide a high-level overview of each structure's functions.
- Appendix B is used to identify SOC services.
- Appendix C is used to identify CSIRT services.

- Appendix D is used to identify SOC and CSIRT common services, and make a selection from the common services for our E-CMIRC.
- Appendix E is dedicated to the development of the E-CMIRC CDM.
- Appendix F is used to develop the E-CMIRC OM. The capability development model and the operations model are then introduced as a single integrated model.
- Appendix G is used to develop the ECMIRC CMM.
- Appendix H provides a National Risk Management Guide. This intention is for nations applying the NCMF to use this guide at level 2 of the NCMF to help with the section and prioritisation process.
- Appendix I offers a NCMF implementation guide.

It needs to be noted again that the primary deliverable of this thesis is the NCMF, and this was done in Part 1 while the E-CMIRC descriptive models in Part 2 is a secondary deliverable. The reader may choose not to read Part 2 with as much attention as Part 1, or even choose not reading it altogether.


Chapter 7: Closure
PART 1
The NCMF
Chapter 2: The NCMF
Chapter 3: The NCMF Level 1
Chapter 4: General Cybersecurity Functions
Chapter 5: The NCMF Level 2 to level 6
Chapter 6: Sample Application of NCMF in SA

# Chapter 7: Closure

## 7.1 Introduction

This study was used to develop an NCMF. The NCMF is a framework that can be used at national level to guide nations during the identification, selection, prioritisation and implementation of national cybersecurity functions. The NCMF is aimed at developing nations, and with the combination of national cybersecurity functions, processes and technologies, developing states may achieve a cost saving. The NCMF is flexible and scalable enough to be used by both developed and developing nations during their national cybersecurity management journey. The rest of this chapter is structured as follows:

**Section 7.2** discusses the research study.

**Section 7.4** provides in tabled format, our problem statement, objectives and deliverables, with an indication on whether we have achieved each of them.

**Section 7.5** discusses future research.

**Section 7.6** summarises the study.

## 7.2 Discussion of the research study



We established that there is a need for a National Cybersecurity Management Framework, as research did not turn up any publicly available frameworks. This led to the development of the National Cybersecurity Management Framework – the NCMF. The intention was to develop the NCMF with a top-down hierarchical approach. The NCMF consists of six levels – starting with level 1 and ending with level 6.

The identification task of the NCMF starts at level 1 and, the selection and prioritisation of cybersecurity functions for implementation is done at level 2. The implementation part of the framework starts at level 3 and ends at level 6. The NCMF satisfies the “plan” part of the PBRM organisational approach. The NCMF level 1 is foundational in nature, and was developed in Chapter 3. Level 1 describes the identification task.

The application of level 1 was illustrated in Chapter 4, where we used it to identify thirteen general cybersecurity functions. The NCMF levels 2 to 6 were developed in Chapter 5. A sample application of the NCMF in the context of South Africa, as a developing country, was provided in Chapter 6.

The management of national cybersecurity consists of four tasks. These tasks are the identification, selection, prioritisation and implementation of national cybersecurity functions. To assist with these cybersecurity

management tasks, we have developed a framework, called the National Cybersecurity Management Framework – the NCMF.

The NCMF has six levels that must be executed sequentially, starting at level 1. Levels 1 to 2 of the NCMF does the identification, selection and prioritisation of cybersecurity functions for implementation at national level. Level 1 has a primary element as well as secondary, influencing elements. The level 1 primary element is:

- **National and international authoritative and normative sources**. These sources prescribe mandatory national cybersecurity functions, or make cybersecurity function recommendations.

The secondary elements influencing and informing the selection and prioritisation of national cybersecurity functions are:

- **Dimensions**. Dimensions are used to identify actors.
- **Domains.** Two possible domains, the offensive and defensive domains.
- **Mandates**. Five different mandates. These are the military cyber, counter cybercrime, intelligence and counter-intelligence, critical information infrastructure protection (ciip) and national crisis management, and cyber diplomacy and internet governance.

Actors involved in national cybersecurity functions are also identified at level 1. To support the identification of actors. We have developed the following templates:



**Level 1 templates**

- Stakeholder and actor identification template.
- Function, structure and actor identification template for domains.

The prioritisation of national cybersecurity functions for implementation happens at level 2. This is achieved by following a national risk management process. For nations that do not have their own national risk management strategy and process, we propose a National Cybersecurity Risk Management Guide in Appendix H.

Level 1 of the NCMF was used to identify thirteen general national cybersecurity functions. Levels 3 to 6 of the NCMF describe the implementation of national cybersecurity functions. The selected and prioritised cybersecurity functions are offered from national cybersecurity structures. To illustrate the application part of the NCMF, we propose a best practice guide in Part 2 for the implementation of a new national cybersecurity structure called the Early Cybersecurity Monitoring and Incident Response Centre (E-CMIRC).

This E-CMIRC structure offers a combination of SOC and CSIRT services to realise a cost benefit. Our intention is for the E-CMIRC to illustrate the implementation part of the NCMF, and also serve as a best practice guide during the development of national cybersecurity structures. The E-CMIRC structure is developed in Part 2, and described with three models in Appendices E to G. These models are:

- E-CMIRC Capability Development Model (E-CMIRC CDM) in Appendix E.
- E-CMIRC Operations Model (E-CMIRC OM) in Appendix F.
- E-CMIRC Capability Maturity Model (E-CMIRC CMM) Appendix G.

We have selected the PBRM organisational approach as a high-level framework to guide the development of the NCMF. The National Cybersecurity Management Framework satisfies the "**p**lan" part of the PBRM organisational approach, while the E-CMIRC, satisfying the **b**uild, **r**un and **m**onitor part of the PBRM organisational approach. In Section 7.3, we will show how we managed to approach the problem statement, objectives and deliverables, and whether we were successful in addressing them.

## 7.3 Problem statement, objective and deliverable mapping

We will use tables to map our problem statement, objectives and deliverables against chapters, and indicate whether we have achieved each of them. We will now in Table 27 show how we solved our problem statement, achieved our objectives and delivered on our deliverables.

**Table 27: Problem statement addressed**

| Problem Statement |
|---|
| A framework, dedicated to developing countries, to assist them with the national cybersecurity management tasks of the:<br><br>• Identification,<br>• Selection,<br>• Prioritisation and<br>• Implementation of national cybersecurity functions could not be identified from the existing literature.<br><br>A developing country specific, initial or start-up national cybersecurity structure - with descriptive models, from where national cybersecurity functions can be offered, could not be identified from the existing literature. It is important to follow a reference framework or model during the execution of national cybersecurity management tasks. Not following a framework or model may lead to disjointed efforts, misalignment between organs of state and state departments, make budgeting difficult, and lead to inconsistent, and non-repeatable results. This ultimately leads to wasted expenditure, and a poor national cybersecurity effort. |

| Section | Artefact | Location | Achieved |
|---|---|---|---|
| Section 1.4 (p29) | The national cybersecurity management framework (NCMF) | Chapter 2 to Chapter 6 | ✓ |
| Section 1.4 (p29) | E-CMIRC | Appendix E to Appendix G | ✓ |
| **Description** | | | |
| The NCMF as a framework was developed to assist both developing and developed nations during the management of national cybersecurity functions. The NCMF provides a mechanism to identify, select, prioritise and implement national cybersecurity functions.<br><br>The E-CMIRC was developed as an initial or start-up national cybersecurity structure. The implementation thereof is described in our best practice guide for the implementation of national cybersecurity structures. | | | |

Table 28 shows that we have achieved our primary objective in Part 1 – Chapters 2 to 6. We have done so through the development of the NCMF. We further show that we have achieved our secondary objective through the development of a best practice guide for the implementation of national cybersecurity structures. We have envisioned a new, initial national cybersecurity structure called the E-CMIRC, and our best practice guide describes the implementation of the E-CMIRC.

**Table 28: Objective addressed**

| Objective | | | |
|---|---|---|---|
| **Primary objective:**<br>To develop a scalable and flexible framework (the NCMF) that can be used by developed and developing countries to<br>• Identify.<br>• Select.<br>• Prioritise.<br>• Implement national cybersecurity functions.<br>**Secondary objective:**<br>To develop a comprehensive best practice guide that may be used during the implementation of national cybersecurity structures. We will develop three models as part of this best practice guide to describe the implementation of national cybersecurity structures. | | | |
| **Section** | **Artefact** | **Location** | **Achieved** |
| Section 1.5 (p30) | **Part 1:** The National Cybersecurity Management Framework (NCMF) | Chapter 2 to Chapter 6 | ✓ |
| Section 1.5 (p30) | **Part 2:** Best practice guide for the implementation of national cybersecurity structures | Appendix A to Appendix G | ✓ |
| **Description** | | | |

**Primary objective - Part 1:** We have met the primary objective by the development of the NCMF. The NCMF is a flexible and scalable framework that can assist nation-states, as well as organisations to identify, select, prioritise and implement national cybersecurity functions.

**Secondary objective - Part 2:** The E-CMIRC was developed as an initial or start-up national cybersecurity structure. The implementation thereof is described in our best practice guide for the implementation of national cybersecurity structures.

In Table 29, we show that we have achieved our two deliverables. The first deliverable is the NCMF framework in Part 1. Our second deliverable in Part 2 is the best practice guide for the implementation of national cybersecurity structures. The implementation of our best practice guide is illustrated through the development of 3 models that describe a newly envisioned national structure called the E-CMIRC.

**Table 29: Deliverables addressed**

| Deliverables | | | |
|---|---|---|---|
| **Primary deliverable**<br>The primary deliverable is a national cybersecurity management framework, the **N**ational **C**ybersecurity **M**anagement **F**ramework (**NCMF**).<br><br>**Secondary deliverable:**<br>The secondary deliverable is a comprehensive **best practice guide that describes the implementation of national cybersecurity structures.** We will describe the implementation of a new structure called the **E**arly **C**ybersecurity **M**onitoring and **I**ncident **R**esponse **C**entre (**E-CMIRC**). It is described using three reference models. | | | |
| **Section** | **Artefact** | **Location** | **Achieved** |
| Section 1.5 (p30) | **Part 1:** The National Cybersecurity Management Framework (NCMF) | Chapters 2 to 6 | ✓ |
| Section 1.5 (p30) | **Part 2:** Best Practice Guide for the Implementation of National Cybersecurity Structures | Appendix A to Appendix G | ✓ |
| **Description** | | | |
| **Primary deliverable – The NCMF in Part 1:** We have met the primary objective by the development of the NCMF. The NCMF is a flexible and scalable framework that can assist nation-states, as well as organisations to identify, select, prioritise and implement national cybersecurity functions.<br><br>**Secondary deliverable – The best practice guide in Part 2:** The best practice guide describes the implementation of a national cybersecurity structure called the E-CMIRC. The focus of this structure is on cost saving, and is aimed at developing countries. The structure is described using three models. | | | |

Table 30 provides a detailed breakdown of the objective and aims of each Chapter and Appendices.

**Table 30: Aims and objectives mapping to parts and chapters**

| Chapter | Objective | Aim | Deliverable |
|---|---|---|---|
| Chapter 1 | Introduce the study, the problem statement and the deliverables. | Introduces the study. | Problem statement<br>Deliverables |
| **Part 1** | | | |
| Chapter 2 | Motivation for an NCMF.<br>• Define functions, services, capabilities and structures.<br>• Introduce authoritative and normative sources<br>• Introduce elements influencing the NCMF<br>• NCMF high-level overview. | Motivate the development of an NCMF.<br>• Establish a common understanding of terms and definitions.<br>• Introduce the NCMF. | NCMF influencing elements |
| Chapter 3 | Development of NCMF level 1. | Ensure all elements influencing the identification of national cybersecurity functions are considered. | NCMF level 1 |
| Chapter 4 | Identify the most general national cybersecurity functions. | Illustrate the application of NCMF level 1 to identify national cybersecurity functions. | Thirteen general cybersecurity functions |
| Chapter 5 | Development of NCMF level 2 to level 6. | Complete and present the NCMF framework. | NCMF level 2 to level 6 |
| Chapter 6 | Illustrate the application of the NCMF in the context of a developing country. | Illustrate to the reader how to apply the NCMF in its entirety in the context of a developing country. | Complete NCMF |
| Chapter 7 | Conclude this study | Justify and close the study. | Conclusion |
| **Part 2** | | | |
| Appendix A | Provide a high-level introduction to SOCs and CSIRTs. | SOCs and CSIRTs were identified as structures whose functions and services can be merged to realise a cost saving. The aim is to orient the reader in terms of the Chapters following. | SOC and CSIRT introduction |
| Appendix B | Determine SOC functions. | Determination of SOC functions. The function complementary services will be determined from these functions. | A list of SOC functions. |
| Appendix C | Determine CSIRT functions. | Determination of CSIRT functions. The function complementary services will be determined from these functions. | A list of CSIRT functions. |
| Appendix D | Determine E-CMIRC functions and services. | The E-CMIRC functions and services are introduced, The E-CMIRC functions and services is a combination of SOC and CSIRT functions and services. | E-CMIRC functions and services. |

| Chapter | Objective | Aim | Deliverable |
|---|---|---|---|
| Appendix E | Development of the E-CMIRC Capability Development Model (E-CMIRC CDM). | Identification of existing capability development models, and selection of a model for the E-CMIRC. | E-CMIRC CDM |
| Appendix F | Development of the E-CMIRC Operations Model (E-CMIRC OM). | Identification of existing operational models, and selection of a model for the E-CMIRC. Presentation of the integrated E-CMIRC CDM and E-CMIRC OM. | E-CMIRC OM and integrated E-CMIRC CDM and OM model. |
| Appendix G | Development of the E-CMIRC Capability Maturity Model (E-CMIRC CMM). | Identification of existing capability maturity models, and selection of a model for the E-CMIRC CMM. Presentation of the E-CMIRC CMM. | E-CMIRC CMM. |
| Appendix H | Development of the national cybersecurity risk management approach | Identifies existing risk management standards and frameworks | National cybersecurity risk management approach |
| Appendix I | NCMF implementation plan | Implementation plan and critical success factors for the implementation of national frameworks. | NCMF implementation plan |

## 7.4 Future research

In future, the E-CMIRC capabilities' measures of effectiveness and measures of performance can be determined. This can augment the E-CMIRC CMM, and allow for the proper benchmarking of cybersecurity services and capabilities at the national level. The NCMF and E-CMIRC could be introduced to developing countries for implementation. This will improve the national cybersecurity posture. Continuous improvement of the NCMF and E-CMIRC will take place, and our framework and models will be benchmarked against existing frameworks, standards and best practices to ensure its currency and usability. It is further important to develop a methodology to evaluate our framework, and future research will focus on developing such an evaluation methodology.



## 7.5 Summary

This study produced a framework to assist nation-states with the identification, selection, prioritisation and implementation of national cybersecurity functions. This framework is called the NCMF, and the application of the NCMF is illustrated with the development of a new national cybersecurity structure – the E-CMIRC.

The E-CMIRC is developed in Part 2 to illustrate the implementation part of the NCMF. The development of the E-CMIRC is done keeping in mind the fiscal and skills constraints of developing countries. The E-CMIRC is described using three models – conforming to the PBRM organisational approach. As deliverables, this study produced the following:

- The NCMF which is a framework to guide, steer and inform the identification and implementation of national cybersecurity functions. The framework follows a top-down hierarchical approach, and consists

of six levels.

- The E-CMIRC structure offering combined cybersecurity services from two national cybersecurity functions – the monitor and evaluate cybersecurity function, and the *incident handling* cybersecurity function. The E-CMIRC is described using three different, models.

    - The E-CMIRC Capability Development Model (E-CMIRC CDM).
    - The E-CMIRC Operations Model (E-CMIRC OM).
    - The E-CMIRC Capability Maturity Model (E-CMIRC CMM).

Using the NCMF to identify national cybersecurity functions will improve the national cybersecurity posture of the nation applying the framework. We have also provided a list of the thirteen most general national cybersecurity functions that nation-states may consider for implementation. Having a secure and dependable ICT infrastructure will foster trust and may facilitate economic activity.

# References


[1] NATO Cooperative Cyber Defence Centre of Excellence, “National Cyber Security Framework Manual,” 2012. [Online]. Available: https://ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf. [Accessed: 24-Nov-2018].

[2] US-Cert, “The National Strategy to Secure Cyberspace,” 2003. [Online]. Available: https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf. [Accessed: 05-Apr-2017].

[3] SITA, “State Information Technology Agency Annual Report 2014 / 2015,” 2015. [Online]. Available: www.sita.co.za/docs/SITA Annual Report 2014-15.pdf. [Accessed: 05-Apr-2017].

[4] Government of Kenya, “Cybersecurity Strategy,” 2014. [Online]. Available: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/KE_NCSS.pdf. [Accessed: 07-Apr-2017].

[5] ngCERT, “National Cybersecurity Strategy,” 2014. [Online]. Available: https://cert.gov.ng/images/uploads/NATIONAL_CYBESECURITY_STRATEGY.pdf. [Accessed: 07-Apr-2017].

[6] SSA, “A National Cybersecurity Policy Framework for South Africa,” 2011. [Online]. Available: https://www.gov.za/documents/national-cybersecurity-policy-framework-4-dec-2015-0000. [Accessed: 20-Dec-2018].

[7] T. Graves, “Service, function and capability,” 2012. [Online]. Available: http://weblog.tetradian.com/2012/09/22/service-function-capability-again/. [Accessed: 02-Jun-2016].

[8] ISO/IEC, “ISO/IEC 27005:2011 Information technology -- Security techniques -- Information security risk management,” 2011. [Online]. Available: http://www.iso.org/iso/catalogue_detail?csnumber=56742. [Accessed: 25-Nov-2018].

[9] C. Furlani, “Managing Information Security Risk: Organization, Mission, and Information System View,” 2011. [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf. [Accessed: 19-Dec-2018].

[10] ISO/IEC, “ISO 31000 - Risk management,” 2009. [Online]. Available: http://www.iso.org/iso/home/standards/iso31000.htm. [Accessed: 19-Dec-2018].

[11] ACM, “ACM Digital Library,” 2016. [Online]. Available: http://dl.acm.org/. [Accessed: 17-Feb-2016].

[12] CiteSeerX, “CiteSeerX,” 2016. [Online]. Available: http://citeseerx.ist.psu.edu/index;jsessionid=165FF246A77A20C39F0FDA9FA0329277. [Accessed: 17-Feb-2016].

[13] Google, “Google Scholar,” 2016. [Online]. Available: https://scholar.google.co.za/. [Accessed: 17-Feb-2016].

[14] IEEE, “IEEE Xplore Digital Library,” 2016. [Online]. Available: http://ieeexplore.ieee.org/Xplore/home.jsp. [Accessed: 17-Feb-2016].

[15] Microsoft, “Microsoft Academic Research,” 2016. [Online]. Available:

http://academic.research.microsoft.com/?SearchDomain=2&entitytype=2. [Accessed: 17-Feb-2016].

[16] BusinessDictionary.com, “Definition of a model,” 2015. [Online]. Available: http://www.businessdictionary.com/definition/model.html. [Accessed: 19-Dec-2018].

[17] Blending Qualitative, “Applying , Testing , and Generating Theories,” *Online*, 2010. [Online]. Available: http://dx.doi.org/10.4135/9781412983525. [Accessed: 19-Dec-2018].

[18] Oxford University Press, “Oxford Advanced Learner’s Dictionary,” 2011. [Online]. Available: http://oald8.oxfordlearnersdictionaries.com/. [Accessed: 25-Nov-2018].

[19] P. Jacobs, “Towards a framework for building security operation centers,” 2015. [Online]. Available: http://research.ict.ru.ac.za/SNRG/Theses/Jacobs 2014 Msc.pdf. [Accessed: 25-Nov-2018].

[20] BusinessDictionary, “What is an organizational structure? definition and meaning - BusinessDictionary.com,” 2018. [Online]. Available: http://www.businessdictionary.com/definition/organizational-structure.html. [Accessed: 04-Jul-2018].

[21] M. Jacobides, “The Inherent Limits of Organizational Structure and the Unfulfilled Role of Hierarchy: Lessons from a Near-War,” *Organ. Sci.*, vol. 18, no. 3, pp. 455–477, Jun. 2007.

[22] J. Wallace, “What is the Purpose of Organizational Structure? | Bizfluent,” 2017. [Online]. Available: https://bizfluent.com/facts-5154174-purpose-organizational-structure.html. [Accessed: 04-Jul-2018].

[23] H. Agarwal; N. Bommadevara & A. Weinberg, “Using a plan-build-run organizational model to drive IT infrastructure objectives | McKinsey & Company,” 2013. [Online]. Available: https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/using-a-plan-build-run-organizational-model-to-drive-it-infrastructure-objectives. [Accessed: 04-Jul-2018].

[24] Y. Zhao, “New Generation IT Operating Model – The Open Group Blog,” 2016. [Online]. Available: https://blog.opengroup.org/2016/02/05/the-new-generation-it-operating-model/. [Accessed: 04-Jul-2018].

[25] BusinessDictionary.com, “Business Function,” 2017. [Online]. Available: http://www.businessdictionary.com/definition/business-function.html. [Accessed: 31-Jan-2017].

[26] BCM Institute, “Business Function,” 2017. [Online]. Available: http://www.bcmpedia.org/wiki/Business_Function. [Accessed: 31-Jan-2017].

[27] Merriam-Webster, “Definition of function,” 2017. [Online]. Available: https://www.merriam-webster.com/dictionary/function. [Accessed: 15-Sep-2017].

[28] BusinessDictionary, “What is a function? definition and meaning - BusinessDictionary.com,” 2018. [Online]. Available: http://www.businessdictionary.com/definition/function.html. [Accessed: 20-Nov-2018].

[29] Dictionary.com, “Synonyms for function,” 2017. [Online]. Available: http://www.thesaurus.com/browse/function. [Accessed: 15-Sep-2017].

[30] R. Heffner, “Business Capability Architecture: Technology Strategy For Business Impact,” 2010. [Online]. Available: http://blogs.forrester.com/enterprise_architecture/2010/02/business-capability-architecture-technology-strategy-for-business-impact.html. [Accessed: 02-Jun-2016].

[31] Merriam-Webster, “Capability,” 2016. [Online]. Available: http://www.merriam-webster.com/dictionary/capability. [Accessed: 07-Oct-2016].

[32] SEBoK, “Capability Engineering,” 2016. [Online]. Available:

http://sebokwiki.org/wiki/Capability_Engineering. [Accessed: 07-Oct-2016].

[33] SSA, “National Cybersecurity Policy Framework,” 2015. [Online]. Available: www.gov.za/sites/www.gov.za/files/39475_gon609.pdf. [Accessed: 25-Nov-2018].

[34] Minister of Justice and Correctional Services, “South African Cybercrimes and Cybersecurity Bill - Draft for Public Comment,” 2015. [Online]. Available: http://www.justice.gov.za/legislation/invitations/CyberCrimesBill2015.pdf. [Accessed: 26-Nov-2015].

[35] South African Government, “Regulation of Interception of Communications and Provision of Communication-Related Information Act, 2002 (Act 70 of 2002),” 2002. [Online]. Available: http://www.acts.co.za/regulation-of-interception-of-communications-and-provision-of-communication-related-information-act-2002/.

[36] Ministry of Information, “Developing National Information Security Strategy for the Kingdom of Saudi Arabia,” 2014. [Online]. Available: http://www.mcit.gov.sa/Ar/MediaCenter/PubReqDocuments/NISS_Draft_7_EN.pdf. [Accessed: 09-Nov-2017].

[37] Freedom House, “Freedom on the Net 2016 - Saudi Arabia Country Profile,” 2016. [Online]. Available: https://freedomhouse.org/report/freedom-net/2016/saudi-arabia. [Accessed: 01-Jan-2017].

[38] S. Azimi, “Iran-Saudi tensions erupt in ‘cyberwar,’” 2016. [Online]. Available: http://www.bbc.com/news/world-middle-east-36438333. [Accessed: 09-Nov-2017].

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

[40] C. Yav, “Legal Frameworks for Data Protection in South Africa and Nigeria,” 2014. [Online]. Available: http://www.centurionlawfirm.com/legal-frameworks-for-data-protection-in-south-africa-and-nigeria/. [Accessed: 02-Sep-2017].

[41] Dictionary.com, “Dimension | Define Dimension at Dictionary.com,” 2018. [Online]. Available: https://www.dictionary.com/browse/dimension?s=t. [Accessed: 14-Aug-2018].

[42] K. Reddy; M. Grobler; I. Swart; R. van Heerden & P. Jacobs, “NCPF Capability Development Report.” Not Published, 2015.

[43] South African Government, “Occupational Health and Safety Act (No. 85 of 1993 ),” 1993. [Online]. Available: http://www.labour.gov.za/DOL/legislation/acts/occupational-health-and-safety/read-online/amended-occupational-health-and-safety-act/. [Accessed: 22-Oct-2017].

[44] FIRST, “About FIRST,” 2005. [Online]. Available: https://www.first.org/about/. [Accessed: 07-Jul-2018].

[45] FIRST, “FIRST Membership Process,” 2005. [Online]. Available: https://www.first.org/membership/process. [Accessed: 07-Jul-2018].

[46] M.N. Schmitt, “Tallinn Manual on the International Law Applicable to Cyber Warfare,” *NATO CCDCOE*, 2013. [Online]. Available: https://ccdcoe.org/tallinn-manual.html.

[47] M. Shaw, “Guides: International and Foreign Cyberspace Law Research Guide: Treaties & International Agreements,” 2018. [Online]. Available: http://guides.ll.georgetown.edu/c.php?g=363530&p=4821478. [Accessed: 09-Jul-2018].

[48] ISO/IEC, “ISO/IEC 27001:2005 Information technology -- Security techniques -- Information security management systems -- Requirements,” 2005. [Online]. Available: http://www.iso.org/iso/catalogue_detail?csnumber=42103.

[49] ISACA, “CoBIT 5 for Information Security,” 2013. [Online]. Available: http://www.isaca.org/COBIT/Documents/COBIT-5-for-Information-Security-Introduction.pdf.

[50] NIST, “NVD - 800-53,” 2018. [Online]. Available: https://nvd.nist.gov/800-53. [Accessed: 09-Jul-2018].

[51] SANS Institute, “Critical Controls for Effective Cyber Defense V 4.1,” 2013. [Online]. Available: http://www.sans.org/critical-security-controls/cag4-1.pdf.

[52] F. Wamala, “The ITU National Cybersecurity Strategy Guide,” *ITU*, 2012. [Online]. Available: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf. [Accessed: 07-Mar-2016].

[53] Roberts T., “Cyber Security Capability Maturity Model (CMM) - Pilot,” *Global Cyber Security Capacity Centre University of Oxford*, 2014. [Online]. Available: https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/cyber-security-capability-maturity-model-cmm. [Accessed: 18-Feb-2016].

[54] K.S. Kumar, “Difference Between Ordinance, Bill, Law and Act,” 2017. [Online]. Available: https://www.linkedin.com/pulse/differences-between-ordinance-bill-law-act-k-satish-kumar-llb-cma/. [Accessed: 07-Mar-2018].

[55] Merriam-Webster, “Dimension,” 2017. [Online]. Available: https://www.merriam-webster.com/dictionary/dimension. [Accessed: 22-Oct-2017].

[56] A. Cockburn, “Writing Effective Use Cases,” 2005. [Online]. Available: http://faculty.washington.edu/stepp/courses/2005spring/tcss360/lectures/notes/02-use_cases.ppt. [Accessed: 04-Mar-2016].

[57] lilzeus, “Stakeholders vs. Actors,” 2003. [Online]. Available: https://www.ibm.com/developerworks/rational/archives/umlcafe/messages/1396.html. [Accessed: 19-Jan-2018].

[58] P. McLeod, “Forums for the Business Analyst,” 2007. [Online]. Available: http://www.modernanalyst.com/Community/Forums/tabid/76/forumid/17/postid/360/scope/posts/Default.aspx. [Accessed: 19-Jan-2018].

[59] F. Serrano, “Use cases: actors vs. stakeholders,” 2014. [Online]. Available: http://fserranocs460.blogspot.com/2014/01/use-cases-actors-vs-stakeholders.html. [Accessed: 19-Jan-2018].

[60] S. James, “Actor v/s Stakeholder,” 2005. [Online]. Available: https://coderanch.com/t/99556/engineering/actor-stakeholder. [Accessed: 19-Jan-2018].

[61] Community Organisers Toolbox, “Understanding Government,” 2017. [Online]. Available: http://www.etu.org.za/toolbox/docs/govern/spheres.html. [Accessed: 19-Jan-2018].

[62] FBI, “Cyber Crime — FBI,” 2018. [Online]. Available: https://www.fbi.gov/investigate/cyber. [Accessed: 17-Aug-2018].

[63] US Department of Homeland Security, “Cybersecurity | Homeland Security,” 2018. [Online]. Available: https://www.dhs.gov/topic/cybersecurity. [Accessed: 17-Aug-2018].

[64] SFIA Foundation, “Why SFIA,” 2015. [Online]. Available: http://www.sfia-online.org/en. [Accessed: 01-

Jul-2016].

[65] NIST, “The National Cybersecurity Workforce Framework,” p. 127, 2013.

[66] R. Brewer, “The six stages of a cyber attack lifecycle - Help Net Security,” 2017. [Online]. Available: https://www.helpnetsecurity.com/2017/03/06/cyber-attack-lifecycle/. [Accessed: 10-Dec-2017].

[67] C. McElroy, “Cyber Security - The Attack Lifecycle - Contegix,” 2015. [Online]. Available: https://www.contegix.com/cyber-security-the-attack-lifecycle/. [Accessed: 10-Dec-2017].

[68] NATO Cooperative Cyber Defence Centre of Excellence, “National Cyber Security Organisation: United Kingdom,” 2015. [Online]. Available: https://ccdcoe.org/multimedia/national-cyber-security-organisation-united-kingdom.html. [Accessed: 19-Sep-2016].

[69] U.S. Nuclear Regulatory Commission, “Cyber Security Programs for Nuclear Facilities,” 2010. [Online]. Available: http://nrc-stp.ornl.gov/slo/regguide571.pdf. [Accessed: 23-Feb-2016].

[70] NIST, “Improving Critical Infrastructure Cybersecurity Executive Order 13636: Preliminary Cybersecurity Framework,” *Nist Standards*, 2013. [Online]. Available: http://www.nist.gov/itl/upload/preliminary-cybersecurity-framework.pdf. [Accessed: 25-Nov-2018].

[71] D. E. Shasha, “Defense in Depth,” *Scientific American*, 2002. [Online]. Available: http://www.nature.com/doifinder/10.1038/scientificamerican0502-101. [Accessed: 25-Nov-2018].

[72] Cichonski P.; Millar T. ; Grance T. & Scarfone K., “Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology, 800-61. Revision 2,” 2012.

[73] ITU, “ITU-T X.1056 - Security incident management guidelines for telecommunications organizations,” 2009. [Online]. Available: http://www.itu.int/rec/T-REC-X.1056-200901-I. [Accessed: 24-Feb-2016].

[74] ISO/IEC, “ISO/IEC 27035:2011 Information technology — Security techniques — Information security incident management,” 2011. [Online]. Available: http://www.iso27001security.com/html/27035.html. [Accessed: 24-Feb-2016].

[75] S. Northcutt, “Security Controls,” 2009. [Online]. Available: http://www.sans.edu/research/security-laboratory/article/security-controls. [Accessed: 03-Dec-2014].

[76] Iowa State Universtity Information Assurance Center, “What is Information Assurance?,” 2016. [Online]. Available: http://www.iac.iastate.edu/. [Accessed: 24-Feb-2016].

[77] Itera, “What is Enterprise Architecture?,” 2016. [Online]. Available: http://www.iteraprocess.com/en/benefits-enterprise-architecture.html. [Accessed: 24-Feb-2016].

[78] The Open Group, “Security Architecture - Developing consistent, reliable standards for secure architectures,” 2016. [Online]. Available: http://www.opengroup.org/subjectareas/security/architecture. [Accessed: 24-Feb-2016].

[79] S. M. Oda, H. Fu, and Y. Zhu, “Enterprise information security architecture a review of frameworks, methodology, and case studies,” *Comput. Sci. Inf. Technol.*, pp. 333–337, 2009.

[80] T. Palmaers, “Implementing a vulnerability management process,” *Information Security*, 2013. [Online]. Available: http://www.sans.org/reading-room/whitepapers/threats/implementing-vulnerability-management-process-34180. [Accessed: 25-Nov-2018].

[81] SEI - Carnegie Mellon, “CSIRT Services,” 2002. [Online]. Available: http://www.cert.org/csirts/services.html. [Accessed: 12-Dec-2015].

[82] DTPS, “Cybersecurity Hub,” 2015. [Online]. Available: https://www.cybersecurityhub.co.za/. [Accessed: 18-Feb-2016].

[83] SSA, “ECS-CSIRT,” 2013. [Online]. Available: http://www.ssa.gov.za/CSIRT.aspx. [Accessed: 18-Feb-2016].

[84] P. Kral and C. Wright, “The Incident Handlers Handbook The Incident Handlers Handbook GIAC (GCIH) Gold Certification.” [Online]. Available: https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901. [Accessed: 16-Feb-2018].

[85] The Business Continuity Institute, “What is BC?,” 2016. [Online]. Available: http://www.thebci.org/index.php/resources/what-is-business-continuity. [Accessed: 11-Nov-2016].

[86] G. Rattray & J. Healey, “Proceedings of a Workshop on Deterring Cyber Attacks,” *Work. Deterring Cyberattacks Informing Strateg. Dev. Options US Policy*, pp. 1–401, 2010.

[87] Meriam-Webster, “Definition of mandate,” 2017. [Online]. Available: https://www.merriam-webster.com/dictionary/mandate. [Accessed: 12-Oct-2017].

[88] World Economic Forum, “Cybercrime | World Economic Forum,” 2018. [Online]. Available: https://www.weforum.org/projects/cybercrime. [Accessed: 25-Jan-2018].

[89] Interpol, “Cybercrime,” 2018. [Online]. Available: https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime. [Accessed: 25-Jan-2018].

[90] Parliament of the Republic of South Africa, “Protection of Critical Infrastructure Bill,” 2015. [Online]. Available: https://jutalaw.co.za/media/filestore/2015/09/PMB4_2015.pdf. [Accessed: 06-Nov-2015].

[91] IAB, “Internet Architecture Board,” 2016. [Online]. Available: https://www.iab.org/. [Accessed: 08-Jun-2017].

[92] IETF, “The Internet Engineering Task Force (IETF®),” 2016. [Online]. Available: https://www.ietf.org/. [Accessed: 23-Feb-2016].

[93] South African Government, “Justice, Crime Prevention and Security Cluster - (JCPS Cluster),” 2017. [Online]. Available: https://www.gov.za/about-government/justice-crime-prevention-and-security-cluster. [Accessed: 15-Oct-2017].

[94] ENISA, “National Cyber Security Strategies (NCSSs) Map — ENISA,” 2018. [Online]. Available: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map. [Accessed: 06-Feb-2018].

[95] Kylie Bull, “Most Countries without Cybersecurity Strategy,” 2017. [Online]. Available: https://www.securitymagazine.com/articles/88281-most-countries-without-cybersecurity-strategy. [Accessed: 16-Nov-2017].

[96] International Labour Office, “A Skilled Workforce for Strong, Sustainable and Balanced Growth: A G20 Training Strategy,” 2011.

[97] Secretariat of the Working Party on Measurement and Analysis of the Digital Economy, “Working Party on Measurement and Analysis of the Digit al Economy,” 2016. [Online]. Available: http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP/IIS(2015)10/FINAL&docLanguage=En. [Accessed: 28-Aug-2017].

[98] Union of International Associations, “The Encyclopedia of World Problems & Human Potential,” 2015. [Online]. Available: http://encyclopedia.uia.org/en/problem/149642. [Accessed: 08-Jun-2017].

[99] FIRST, “Education Program: Services Framework,” 2017. [Online]. Available: https://www.first.org/education/service-framework. [Accessed: 25-Nov-2018].

[100] F. Wamala, “ITU Nationall Cyber security strategy guide,” *ITU*, 2012. [Online]. Available: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf. [Accessed: 18-Feb-2016].

[101] Christopher J.D., “Cybersecurity Capability Maturity Model (C2M2) Program,” *Department of Homeland Security*, 2014. [Online]. Available: http://energy.gov/oe/services/cybersecurity/cybersecurity-capability-maturity-model-c2m2-program. [Accessed: 25-Nov-2018].

[102] UK Government, “National Cyber Security Strategy 2016-2021,” 2016. [Online]. Available: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national_cyber_security_strategy_2016.pdf. [Accessed: 06-Feb-2018].

[103] Irish Government, “Irish National Cyber Security Strategy,” 2015. [Online]. Available: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS_IE.pdf. [Accessed: 06-Feb-2018].

[104] German Federal Government, “Cyber Security Strategy for Germany,” 2011. [Online]. Available: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Germancybersecuritystrategy20111.pdf. [Accessed: 06-Feb-2018].

[105] Slovak Republic, “Cyber Security Concept of the Slovak Republic,” 2015. [Online]. Available: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/cyber-security-concept-of-the-slovak-republic-1. [Accessed: 06-Feb-2018].

[106] Finnish Government, “Finland´s Cyber Strategy www.yhteiskunnanturvallisuus.fi,” 2013. [Online]. Available: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/FinlandsCyberSecurityStrategy.pdf. [Accessed: 06-Feb-2018].

[107] Cisco, “Internet of Things (IoT) - Cisco.” [Online]. Available: https://www.cisco.com/c/en/us/solutions/internet-of-things/overview.html. [Accessed: 16-Feb-2018].

[108] R. A. Clarke & R. Knake, *Cyber War: The Next Threat to National Security and What to Do About It, Ecco, 2011*. Ecco; Reprint edition (August 5, 2011), 2012.

[109] SABC, “Annual Report 2014/2015,” 2015. [Online]. Available: http://www.sabc.co.za/sabc/annual-reports/. [Accessed: 25-Nov-2018].

[110] South African Parliament, “South African Parliamentary Q&A Session - SACSA,” 2003. [Online]. Available: https://cryptome.org/za-crypto.htm. [Accessed: 20-Apr-2017].

[111] International Telecommunication Union, “Global Cybersecurity Index (GCI) 2017,” 2017.

[112] DTPS, “Independent Communications Authority of South Africa (ICASA),” 2016. [Online]. Available: http://www.dtps.gov.za/independent-communications-authority-of-south-africa-icasa.html. [Accessed: 29-Feb-2016].

[113] ICASA, “ICASA,” 2016. [Online]. Available: https://www.icasa.org.za/. [Accessed: 29-Feb-2016].

[114] NERSA, “NERSA,” 2016. [Online]. Available: http://www.nersa.org.za/. [Accessed: 29-Feb-2016].

[115] BusinessDictionary, “Regulatory Agency Listings,” 2008. [Online]. Available: http://www.businessdictionary.com/definition/regulatory-agency.html. [Accessed: 08-Sep-2017].

[116] T. Boshoff, “Summary of OHS ACT Regulations | Labour Guide,” 2018. [Online]. Available: http://www.labourguide.co.za/health-and-safety/1502-summary-of-ohs-act-regulations. [Accessed: 11-Feb-2018].

[117] P. C. Jacobs, S. H. von Solms, and M. M. Grobler, “Towards a framework for the development of business cybersecurity capabilities,” *Bus. Manag. Rev.*, vol. 7, no. 4, pp. 51–61, 2016.

[118] South African Government, “Electronic Communications and Transactions Act, 2002 (Act No. 25 of 2002),” 2002. [Online]. Available: http://www.acts.co.za/electronic-communications-and-transactions-act-2002/. [Accessed: 29-Feb-2016].

[119] DPSA, “Public Service Corporate Governance of Information and Communication Technology Policy Framework,” 2012. [Online]. Available: http://www.gov.za/sites/www.gov.za/files/CGICTPolicyFramework.pdf. [Accessed: 25-Nov-2018].

[120] M. Czernowalow, “Cyber response group to develop policy,” 2014. [Online]. Available: http://www.itweb.co.za/index.php?option=com_content&view=article&id=139125. [Accessed: 13-Apr-2017].

[121] IT News Africa, “South Africa launches National Cyber Security Advisory Council,” 2013. [Online]. Available: http://www.itnewsafrica.com/2013/10/south-africa-launches-national-cyber-security-advisory-council/. [Accessed: 25-Nov-2018].

[122] DTPS, “Minister Inaugurates National Cyber Security Advisory Council,” 2013. [Online]. Available: https://www.dtps.gov.za/index.php?option=com_content&view=article&id=247:minister-inaugurates-national-cyber-security-advisory-council&catid=13&Itemid=138. [Accessed: 08-Sep-2017].

[123] ISO/IEC, “ISO/IEC 27005:2008 Information security risk management_,” 2011. [Online]. Available: http://www.iso.org/iso/catalogue_detail?csnumber=42107. [Accessed: 25-Nov-2018].

[124] M. Shinn, “Cybersecurity: Department & SABRIC briefing, with Deputy Minister present,” 2017. [Online]. Available: https://pmg.org.za/committee-meeting/24042/. [Accessed: 08-Sep-2017].

[125] DTPS, “SECTOR CSIRTs,” 2017. [Online]. Available: https://www.cybersecurityhub.gov.za/sector-csirt. [Accessed: 08-Sep-2017].

[126] General Secretariat of the Organization of American States (OAS) and Organization of American States, “Best Practices for Establishing a National CSIRT,” 2016. [Online]. Available: https://www.sites.oas.org/cyber/Documents/2016 - Best Practices CSIRT.pdf. [Accessed: 29-Jul-2016].

[127] W. Huang; K. Siau & K.K. Wei, “Electronic Government Strategies and Implementation,” 2005. [Online]. Available: https://books.google.nl/books?hl=en&lr=&id=d84laQpqb1QC&oi=fnd&pg=PP1&dq=Electronic+Government+Strategies+and+Implementation&ots=hJhjoWPgk2&sig=iwCCRTsJ_gKCI8oMlMwRyjCsmVc#v=onepage&q=Electronic Government Strategies and Implementation&f=false. [Accessed: 25-Nov-2018].

[128] Tripwire, “ISO 27001 Compliance: Security is Standard with Tripwire,” 2013. [Online]. Available: http://www.tripwire.com/regulatory-compliance/iso-27001/. [Accessed: 25-Nov-2018].

[129] ISACA, “COBIT 5 Framework,” 2016. [Online]. Available: https://www.isaca.org/cobit/pages/cobit-5-framework-product-page.aspx. [Accessed: 29-May-2017].

[130] South African Government, “South African Police Service Act, 1995 (Act No. 68 of 1995),” 1995. [Online]. Available: https://www.acts.co.za/south-african-police-service-act-1995/index.html. [Accessed: 22-Oct-2017].

[131] M. Avenant, “Deloitte opens first African Cyber Intelligence Centre,” 2016. [Online]. Available: http://www.itweb.co.za/index.php?option=com_content&view=article&id=153333. [Accessed: 02-May-2017].

[132] T. McGuiness, “Defense In Depth,” 2001. [Online]. Available: https://www.sans.org/reading-room/whitepapers/basics/defense-in-depth-525. [Accessed: 22-Feb-2018].

[133] J. Shenk, “SANS Seventh Annual Log Management Survey Report,” 2011. [Online]. Available: http://www.sans.org/reading_room/analysts_program/logmgt-survey-web.pdf. [Accessed: 25-Nov-2018].

[134] M. Adler, “CoBIT 4.1,” 2007. [Online]. Available: https://www.isaca.org/Knowledge-Center/cobit/Documents/COBIT4.pdf. [Accessed: 25-Nov-2018].

[135] J. Heschl & G. Hardy, “Aligning COBIT 4.1, ITIL V3 and ISO/IEC 27002 for Business Benefit,” 2008. [Online]. Available: https://www.isaca.org/Knowledge-Center/Research/Documents/Aligning-COBIT-ITIL-V3-ISO27002-for-Business-Benefit_res_Eng_1108.pdf. [Accessed: 25-Nov-2018].

[136] R.S. Ross, “Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans,” *NIST Special Publication*, 2014. [Online]. Available: papers3://publication/doi/10.6028/NIST.SP.800-53Ar4. [Accessed: 16-Mar-2016].

[137] 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. [Accessed: 26-Nov-2014].

[138] P. Jacobs, “Towards a framework for building security operation centers,” 2015. [Online]. Available: http://contentpro.seals.ac.za/iii/cpro/DigitalItemViewPage.external?lang=eng&sp=1017932&sp=T&suite=def. [Accessed: 25-Nov-2018].

[139] ITIL, “Incident Management,” 2011. [Online]. Available: http://wiki.en.it-processmaps.com/index.php/Incident_Management. [Accessed: 05-Jun-2015].

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

[141] SEI at Carnegie Mellon University, “CERT Division Frequently Asked Questions (FAQ),” 2015. [Online]. Available: http://www.cert.org/faq/. [Accessed: 18-May-2015].

[142] R. Ruefle, “Defining Computer Security Incident Response Teams,” 2007. [Online]. Available: http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=294557. [Accessed: 13-Jan-2016].

[143] ENISA and CMU SEI, “CSIRT Services,” 2016. [Online]. Available: http://www.cert.org/incident-management/services.cfm? [Accessed: 01-Jan-2016].

[144] J.Wiik; J.J. Gonzalez; & K.P. Kossakowski, “Effectiveness of Proactive CSIRT services,” 2006. [Online]. Available: https://www.first.org/conference/2006/papers/kossakowski-klaus-papers.pdf. [Accessed: 03-Sep-2016].

[145] G. Killcreses; K. Kossakowski; R. Ruefle; M. Zajicek, “Organizational Models for Computer Security

Incident Response Teams (CSIRTs),” 2003. [Online]. Available: www.sei.cmu.edu/reports/03hb001.pdf. [Accessed: 30-Jun-2016].

[146] Killcrece G. et al, “State of the Practice of Computer Security Incident Response Teams (CSIRTs),” 2003. [Online]. Available: http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=6571. [Accessed: 07-Jan-2016].

[147] A. Tagert, “Cybersecurity Challenges in Developing Nations,” 2010. [Online]. Available: https://pdfs.semanticscholar.org/f7e0/eb22e3ad85754ff90b18e26cf4aa120e73be.pdf. [Accessed: 25-Nov-2018].

[148] ENISA, “Definition of a CSIRT,” 2015. [Online]. Available: https://www.enisa.europa.eu/activities/cert/support/guide/strategy/what-is-csirt/definition. [Accessed: 24-Nov-2015].

[149] R. Morgus; I. Skierka; M. Hohmann & T. Maurer, “National CSIRTs and Their Role in Computer Security Incident Response,” 2015. [Online]. Available: http://www.digitaldebates.org/fileadmin/media/cyber/National_CSIRTs_and_Their_Role_in_Computer_Security_Incident_Response__November_2015_--_Morgus__Skierka__Hohmann__Maurer.pdf. [Accessed: 25-Nov-2018].

[150] J. Haller; S.A. Merrel; M.J. Butcivic & B.J. Willke, “Best Practices for National Cyber Security: Building a National Computer Security Incident Management Capability,” 2011.

[151] B. Kaskina; E. Taurins; A. Dufkova, “CSIRT Capabilities How to assess maturity?,” 2015. .

[152] R. Ruefle, “Defining Computer Security Incident Response Teams | US-CERT,” 2007. [Online]. Available: https://www.us-cert.gov/bsi/articles/best-practices/incident-management/defining-computer-security-incident-response-teams. [Accessed: 26-Feb-2018].

[153] Standard Bank, “Standard Bank,” 2016. [Online]. Available: http://www.standardbank.co.za/standardbank/. [Accessed: 20-Sep-2016].

[154] G. van Zyl, “Standard Bank computer was hacked in R300m ATM fraud hit - report,” 2016. [Online]. Available: http://www.fin24.com/Tech/Cyber-Security/standard-bank-computer-was-hacked-in-r300m-atm-fraud-hit-report-20160630. [Accessed: 20-Sep-2016].

[155] M. Peacock, “IT Service Delivery Model Overview,” 2009. [Online]. Available: https://www.slideshare.net/peacock.ma/it-service-delivery-model-overview. [Accessed: 10-Mar-2018].

[156] U. Kannan, “Which IT Service Delivery Model is right for your organisation? - Open Dialog - Dialog Information Technology,” 2018. [Online]. Available: https://www.dialog.com.au/open-dialog/which-it-service-delivery-model-is-right-for-your-organisation/. [Accessed: 10-Mar-2018].

[157] I. Roth, “ITIL Overview,” 2008. [Online]. Available: http://www.itilcertification.org/.

[158] Torres A., “Building a World-Class Security Operations Center: A Roadmap,” 2015. [Online]. Available: https://www.sans.org/reading-room/whitepapers/analyst/building-world-class-security-operations-center-roadmap-35907. [Accessed: 17-Nov-2015].

[159] E. Zhang, “How to Build a Security Operations Center (SOC): Peoples, Processes, and Technologies,” 2018. [Online]. Available: https://digitalguardian.com/blog/how-build-security-operations-center-soc-peoples-processes-and-technologies. [Accessed: 21-Feb-2018].

[160] C. Crowley, “Future SOC: SANS 2017 Security Operations Center Survey,” 2017. [Online]. Available:

https://www.sans.org/reading-room/whitepapers/analyst/future-soc-2017-security-operations-center-survey-37785. [Accessed: 21-Feb-2018].

[161] P. Paganini, “What is a SOC?,” 2016. [Online]. Available: http://securityaffairs.co/wordpress/47631/breaking-news/soc-security-operations-center.html. [Accessed: 20-Sep-2016].

[162] M. Rouse, “What is security information and event management (SIEM)? - Definition from WhatIs.com,” 2014. [Online]. Available: http://searchsecurity.techtarget.com/definition/security-information-and-event-management-SIEM. [Accessed: 21-Feb-2018].

[163] J.P. Mello, “SIEM tools: Essential features for a SOC organization | Learn,” 2017. [Online]. Available: https://learn.techbeacon.com/units/siem-tools-essential-features-soc-organization. [Accessed: 21-Feb-2018].

[164] Gartner, “Managed Security Service Provider (MSSP),” 2013. [Online]. Available: http://www.gartner.com/it-glossary/mssp-managed-security-service-provider. [Accessed: 17-Nov-2015].

[165] DarkReading, “How To Pick The Best MSSP For Your SMB,” 2013. [Online]. Available: https://www.darkreading.com/risk/how-to-pick-the-best-mssp-for-your-smb/d/d-id/1138968. [Accessed: 25-Nov-2018].

[166] KISA, “Korea Internet and Security Agency,” 2016. [Online]. Available: https://www.kisa.or.kr/eng/main.jsp. [Accessed: 20-Sep-2016].

[167] P. Jacobs; A. Arnab & B.Irwin, “Classification of Security Operation Centers,” in *Information Security for South Africa, 2013*, 2013, pp. 1–7.

[168] SITA, “SITA Annual Report 2011/2012,” 2012. [Online]. Available: http://rfq.sita.co.za/docs/SITA_AR_2012___web.pdf. [Accessed: 25-Nov-2018].

[169] H. Vlavianos, *Emerging Critical Technologies and Security in the Asia-Pacific*, 1st ed. London: Palgrave Macmillan UK, 2016.

[170] B. Rothke, “Building a Security Operations Center (SOC),” *RSA Conference Europe 2009*, 2009. [Online]. Available: https://www.rsaconference.com/events/us12/agenda/sessions/683/building-a-security-operations-center-soc. [Accessed: 19-Dec-2018].

[171] B. Rothke, “Building a Security Operations Center (SOC),” 2012. [Online]. Available: https://www.rsaconference.com/events/us12/agenda/sessions/683/building-a-security-operations-center-soc. [Accessed: 04-Jun-2014].

[172] A. Chuvakin, “Selecting and Deploying SaaS SIEM for Security Monitoring,” 2017. [Online]. Available: https://www.gartner.com/document/3822563. [Accessed: 21-Feb-2018].

[173] F. Siemons, “SIEM as a Service,” 2016. [Online]. Available: http://resources.infosecinstitute.com/siem-as-a-service/. [Accessed: 21-Feb-2018].

[174] KPMG, “Security operations center (SOC) globalization,” 2012. [Online]. Available: http://www.kpmg.com/SG/en/IssuesAndInsights/ArticlesPublications/Documents/Advisory-CS-Security-Operations-Center-SOC-Globalization.pdf. [Accessed: 04-Jun-2015].

[175] ISACA, “Incident Management and Response,” 2012. [Online]. Available: http://www.isaca.org/knowledge-center/research/researchdeliverables/pages/incident-management-

and-response.aspx. [Accessed: 26-Apr-2016].

[176] J. Wang, “Anatomy of a Security Operations Center,” 2010. [Online]. Available: https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20110011188.pdf. [Accessed: 25-Nov-2018].

[177] PCI Security Standards Council, “Payment Card Industry ( PCI ) Data Security Standards Overview,” 2010. [Online]. Available: https://www.pcisecuritystandards.org/security_standards/. [Accessed: 25-Nov-2018].

[178] ISO/IEC, “An Introduction to ISO 27001, ISO 27002....ISO 27008,” 2009. [Online]. Available: http://www.27000.org/. [Accessed: 25-Nov-2018].

[179] United States Government, “The Sarbanes-Oxley Act of 2002,” 2002. [Online]. Available: http://www.soxlaw.com/s404.htm. [Accessed: 25-Nov-2018].

[180] D. Swift, “Successful SIEM and Log Management Strategies for Audit and Compliance,” 2010. .

[181] D. Kelley & R. Morits, “Best Practices for Building a Security Operations Center,” *(ISC)2 Inf. Syst. Secur.*, vol. 14, no. 6, pp. 27–32, 2006.

[182] J. Milne, “Build Your Own Security Operations Center,” *InformationWeek*, 2005. [Online]. Available: https://www.slideshare.net/ahmadhagh/an-introduction-to-soc-security-operation-center. [Accessed: 25-Nov-2018].

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

[184] Bancroft S. et al, “CISO Information Security Workshop,” 2016. [Online]. Available: https://books.google.nl/books?id=ijaeDAAAQBAJ&pg=PA351&lpg=PA351&dq=%22CISO+Information+Security+Workshop%22+bancroft&source=bl&ots=51hVn6SVRY&sig=g7bV-siPpg5L1-TbzotQgC5L9rI&hl=en&sa=X&ved=2ahUKEwi-1Yr_9e7eAhVSyhoKHf5HBUQQ6AEwB3oECAEQAQ#v=onepage&q=%22CI. [Accessed: 25-Nov-2018].

[185] C. Zimmerman, “Ten Strategies of a World-Class Cybersecurity Operations Center,” 2014. [Online]. Available: https://www.mitre.org/sites/default/files/publications/pr-13-1028-mitre-10-strategies-cyber-ops-center.pdf. [Accessed: 25-Nov-2018].

[186] D. Kelley & R. Moritz, “Best Practices for Building a Security Operations Center,” *Inf. Syst. Secur.*, vol. 14, no. 6, pp. 27–32, 2006.

[187] J. Bevis, “Creating and Maintaining a SOC - The details behind successful Security Operations Centers,” 2012. [Online]. Available: http://www.mcafee.com/us/resources/white-papers/foundstone/wp-creating-maintaining-soc.pdf. [Accessed: 25-Nov-2018].

[188] B. Anderson, “Building, Maturing & Rocking a Security Operations Center,” *SANS Institute*, 2011. [Online]. Available: https://www.sans.org/summit-archives/file/summit-archive-1493741010.pdf. [Accessed: 25-Nov-2018].

[189] IBM, “The 5 essential functions of an enterprise security operations center (SOC),” 2016. [Online]. Available: http://www-935.ibm.com/services/us/en/it-services/security-services/the-five-essential-functions-of-an-enterprise-security-operations-center-infographic/. [Accessed: 26-May-2015].

[190] P. Jacobs; S.H. von Solms & M.M. Grobler, “E-CMIRC – Towards a model for the integration of services between SOCs and CSIRTs,” in *Proceedings of The 15th European Conference on Cyber*

*Warfare and Security*, 2016, p. 350.

[191] M. Z. M. J. West-Brown, D. Stikvoort, K. Kossakowski, G. Killcrece, R. Ruefle, “Handbook for Computer Security Incident Response Teams (CSIRTs),” 2003. [Online]. Available: http://resources.sei.cmu.edu/asset_files/Handbook/2003_002_001_14102.pdf. [Accessed: 25-Nov-2018].

[192] A. Dufkova, “CERT Community Recognition mechanisms and schemes,” 2013. [Online]. Available: https://www.enisa.europa.eu/activities/cert/support/baseline-capabilities/cert-community-recognition-mechanisms-and-schemes/at_download/fullReport. [Accessed: 24-Aug-2016].

[193] ENISA, “CSIRT Structure,” 2015. .

[194] Software Engineering Institute, “CSIRT Frequently Asked Questions (FAQ),” 2016. [Online]. Available: https://www.cert.org/incident-management/csirt-development/csirt-faq.cfm? [Accessed: 01-Jun-2016].

[195] I. Skierka; R. Morgus; M. Hohmann & T. Maurer, “CSIRT Basics for Policy-Makers,” 2015. [Online]. Available: http://www.gppi.net/fileadmin/user_upload/media/pub/2015/CSIRT_Basics_for_Policy-Makers_May_2015_WEB.pdf. [Accessed: 24-Aug-2016].

[196] SABRIC, “About Us,” 2016. [Online]. Available: https://www.sabric.co.za/about-us/. [Accessed: 15-Aug-2016].

[197] N. Brownlee, “Expectations for Computer Security Incident Response,” *IETF RFC 2350*, 1998. [Online]. Available: http://www.ietf.org/rfc/rfc2350.txt. [Accessed: 25-Nov-2018].

[198] 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. [Accessed: 22-May-2017].

[199] B. J. W. J. Haller, S.A. merrell, M.J. Butkovic, “Best Practices for National Cyber Security: Building a National Computer Security Incident Management Capability, Version 2.0,” 2011. [Online]. Available: https://resources.sei.cmu.edu/asset_files/TechnicalReport/2011_005_001_15401.pdf. [Accessed: 26-Feb-2018].

[200] C. Bronk, *Cyber threat : the rise of information geopolitics in U.S. national security*. ABC-CLIO, LLC, 2016.

[201] O. Kruidhof, “Evolution of National and Corporate CERTs - Trust, the Key Factor,” 2014. [Online]. Available: https://pdfs.semanticscholar.org/f586/131329f4842bae5e74bae77adea783eb993e.pdf. [Accessed: 25-Nov-2018].

[202] Dell, “Security Operations Centers,” 2013. [Online]. Available: http://www.secureworks.com/it_security_services/advantage/soc/. [Accessed: 25-Nov-2018].

[203] DTS Solution, “Security Operations Center 2.0,” 2015. [Online]. Available: http://www.dts-solution.com/solutions/security-operations-center/. [Accessed: 25-Nov-2018].

[204] HCLTech, “HCL Managed Security Services -Security Operations Made Simpler,” 2014. [Online]. Available: http://www.hcltech.com/it-infrastructure-management/managed-security-services. [Accessed: 25-Nov-2018].

[205] Hewlett-Packard, “5G/SOC: SOC Generations,” 2013. [Online]. Available:

http://www.cnmeonline.com/myresources/hpe/docs/HP_ArcSight_WhitePapers_5GSOC_SOC_Generations.PDF. [Accessed: 25-Nov-2018].

[206] IBM, “Virtual Security Operations Center (SOC),” 2104. [Online]. Available: https://www.ibm.com/security/services/virtual-security-operations-center-soc. [Accessed: 26-Nov-2018].

[207] McAfee, “Case Study McAfee’s Unique Prevent-Detect-Respond Approach and Security Operations Center Showcase Best Practices,” 2013. [Online]. Available: https://www.mcafee.com/enterprise/en-us/security-awareness/operations/what-is-soc.html. [Accessed: 26-Nov-2018].

[208] Neusoft, “NetEye Security Operations Center (SOC),” 2015. [Online]. Available: http://www.neusoft.com/products&platform/1338/. [Accessed: 26-Nov-2018].

[209] SecureOps, “SecureOps Security Operations Center,” 2013. [Online]. Available: http://secureops.com/Services/Monitoring-Services.html. [Accessed: 26-Nov-2018].

[210] Symantec, “Symantec Unveils New Global Security Operations Center in U.S.,” 2012. [Online]. Available: https://www.symantec.com/about/newsroom/press-releases/2012/symantec_0207_01. [Accessed: 26-Nov-2018].

[211] T-Systems, “Security,” 2013. [Online]. Available: https://www.t-systems.com/sg/en/solutions/security/security-topics/networks/network-security-428916. [Accessed: 26-Nov-2018].

[212] Dictionary of Military and Associated Terms, “Cyber counterintelligence,” 2005. [Online]. Available: https://www.thefreedictionary.com/_/cite.aspx?url=https%3A%2F%2Fwww.thefreedictionary.com%2Fcyber%2Bcounterintelligence&word=cyber counterintelligence&sources=mili. [Accessed: 14-Mar-2018].

[213] M. Tremblay, “Cyber-Surveillance,” 2012. [Online]. Available: http://www.dictionnaire.enap.ca/dictionnaire/docs/definitions/definitions_anglais/cyber_surveillance.pdf. [Accessed: 26-Nov-2018].

[214] Gartner, “Threat Intelligence: What is it, and How Can it Protect You from Today’s Advanced Cyber-Attacks?,” 2014. [Online]. Available: https://www.gartner.com/imagesrv/media-products/pdf/webroot/issue1_webroot.pdf. [Accessed: 14-Mar-2018].

[215] Office of Government Commerce, “ITIL,” 2000. [Online]. Available: http://www.itil-officialsite.com/. [Accessed: 26-Nov-2018].

[216] ITU-T, “Incident organization and security incident handling: Guidelines for telecommunication organizations,” *ITU-T Recommendation E.409*, 2004. [Online]. Available: https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-E.409-200405-I!!PDF-E&type=items. [Accessed: 26-Apr-2016].

[217] Praxiom Research Group, “ISO 27000 Infosec Definitions,” 2016. [Online]. Available: http://www.praxiom.com/iso-27000-definitions.htm#Information_security_incident. [Accessed: 02-Aug-2016].

[218] ITIL, “ITIL Definition: Asset Management (v2, v3),” 2018. [Online]. Available: http://www.knowledgetransfer.net/dictionary/ITIL/en/Asset_Management.htm. [Accessed: 14-Mar-2018].

[219] IAITAM, “What is IT Asset Management? Let IAITAM be your guide.,” 2018. [Online]. Available: http://iaitam.org/what-is-it-asset-management/. [Accessed: 14-Mar-2018].

[220] Businessdictionary, “What is analysis? definition and meaning - BusinessDictionary.com,” 2018. [Online]. Available: http://www.businessdictionary.com/definition/analysis.html. [Accessed: 14-Mar-2018].

[221] Merriam-Webster, “Aggregate | Definition of Aggregate by Merriam-Webster,” 2018. [Online]. Available: https://www.merriam-webster.com/dictionary/aggregate. [Accessed: 14-Mar-2018].

[222] I. Wigmore, “What is correlation? - Definition from WhatIs.com,” 2016. [Online]. Available: http://whatis.techtarget.com/definition/correlation. [Accessed: 14-Mar-2018].

[223] PNMSoft, “Digital Workflow Tutorial - What is a Workflow?,” 2016. [Online]. Available: http://www.pnmsoft.com/resources/bpm-tutorial/workflow-tutorial/. [Accessed: 15-Mar-2018].

[224] Techopedia, “What is Digital Forensics? - Definition from Techopedia,” 2018. [Online]. Available: https://www.techopedia.com/definition/27805/digital-forensics. [Accessed: 15-Mar-2018].

[225] Merriam-Webster, “Research | Definition of Research by Merriam-Webster,” 2018. [Online]. Available: https://www.merriam-webster.com/dictionary/research. [Accessed: 15-Mar-2018].

[226] Georgia Tech Institute for Information Security & privacy, “Cybersecurity Research Underway | Institute for Information Security & Privacy | Georgia Tech,” 2018. [Online]. Available: https://iisp.gatech.edu/research. [Accessed: 15-Mar-2018].

[227] T. Palmaers, “Implementing a Vulnerability Management Process,” 2013. [Online]. Available: https://www.sans.org/reading-room/whitepapers/threats/implementing-vulnerability-management-process-34180. [Accessed: 15-Mar-2018].

[228] Techopedia, “What is IT Risk Management? - Definition from Techopedia,” 2018. [Online]. Available: https://www.techopedia.com/definition/25836/it-risk-management. [Accessed: 15-Mar-2018].

[229] European Network and Information Security Agency and (ENISA), “CSIRT Services,” 2015. [Online]. Available: https://www.enisa.europa.eu/activities/cert/support/guide/appendix/csirt-services. [Accessed: 01-Jun-2015].

[230] SEI at CMU, “CSIRT SERVICES,” 2017. [Online]. Available: https://resources.sei.cmu.edu/asset_files/WhitePaper/2002_019_001_53048.pdf. [Accessed: 15-Mar-2018].

[231] M.K.G. Adomey, “Introduction to Computer Security Incident Response Team (CSIRT),” 2016. [Online]. Available: https://www.itu.int/en/ITU-D/.../Session 2 -1115-1230-v09-10-2016.pdf. [Accessed: 22-May-2017].

[232] Arcsight, “Building a Successful Security Operations Center,” 2009. [Online]. Available: http://www.scribd.com/doc/39599055/ArcSight-Whitepaper-SuccessfulSOC. [Accessed: 13-Apr-2015].

[233] McAfee, “Focus on 5 SIEM Requirements,” 2012. [Online]. Available: https://www.mcafee.com/enterprise/en-us/assets/solution-briefs/sb-focus-on-five-siem-requirements.pdf. [Accessed: 26-Nov-2018].

[234] SEI, “Creating and Managing Computer Security Incident Handling Teams (CSIRTs).” [Online]. Available: https://www.first.org/conference/2008/papers/killcrece-georgia-slides.pdf. [Accessed: 26-

Nov-2018].

[235] NIST, “Cyber Security Framework,” 2014. [Online]. Available: http://www.nist.gov/cyberframework/.

[236] ISO, “ISO/IEC 27005:2011 Information security risk management,” 2011. [Online]. Available: http://www.iso.org/iso/catalogue_detail?csnumber=56742. [Accessed: 25-Nov-2018].

[237] T. Olzak, “The elements of business continuity planning,” *TechRepublic*, 2013. [Online]. Available: http://www.techrepublic.com/blog/data-center/the-elements-of-business-continuity-planning/. [Accessed: 26-Nov-2018].

[238] Secure IT Foundation, “Diginotar Disaster Explained.” [Online]. Available: http://secureitfoundation.wordpress.com/2011/09/07/diginotar-debarcle-explained/. [Accessed: 26-Nov-2018].

[239] ISO/IEC, “ISO 22301:2012 Societal security -- Business continuity management systems --- Requirements,” 2012. [Online]. Available: https://www.iso.org/standard/50038.html. [Accessed: 23-May-2017].

[240] SEI at CMU, “List of National CSIRTs,” 2016. [Online]. Available: http://www.cert.org/incident-management/national-csirts/national-csirts.cfm? [Accessed: 22-Sep-2016].

[241] ENISA, “CSIRTs by Country - Interactive Map,” 2016. [Online]. Available: https://www.enisa.europa.eu/topics/national-csirt-network/csirt-inventory/certs-by-country-interactive-map. [Accessed: 22-Sep-2016].

[242] N. Shafqat and A. Masood, “Comparative Analysis of Various National Cyber Security Strategies,” *Int. J. Comput. Sci. Inf. Secur.*, vol. 14, no. 1, pp. 129–136, 2016.

[243] C. Office, “Cyber Security Strategy,” 2011. [Online]. Available: http://webarchive.nationalarchives.gov.uk/20120404150643/http://cabinetoffice.gov.uk/resource-library/cyber-security-strategy. [Accessed: 17-Aug-2016].

[244] S. Song, “African Undersea Cables,” 2016. [Online]. Available: https://www.flickr.com/photos/ssong/27665889970/. [Accessed: 23-Sep-2016].

[245] PriMetrica Inc, “Submarine Cable Map,” 2016. [Online]. Available: http://www.submarinecablemap.com/#/landing-point/melkbosstrand-south-africa. [Accessed: 23-Sep-2016].

[246] ISPA, “Internet Exchange,” 2016. [Online]. Available: http://ispa.org.za/inx/. [Accessed: 23-Sep-2016].

[247] “INX Locations and Information,” 2016. [Online]. Available: https://wiki.inx.net.za/display/pub/INX+Locations+and+Information. [Accessed: 23-Sep-2016].

[248] IXP Toolkit, “South Africa,” 2015. [Online]. Available: http://ixptoolkit.org/content/south-africa. [Accessed: 27-Sep-2016].

[249] R. Muller, “Telkom, Vodacom peering at JINX, CINX: the battle continues,” 2012. [Online]. Available: http://mybroadband.co.za/news/internet/60225-telkom-vodacom-peering-at-jinx-cinx-the-battle-continues.html. [Accessed: 27-Sep-2016].

[250] C. Lawson; A. Hils & C. Neiva, “Magic Quadrant for Intrusion Prevention Systems.” [Online]. Available: http://www.ts.avnet.com/it/magic. [Accessed: 27-Sep-2016].

[251] B. van Niekerk & P. Jacobs, “Toward a Secure Data Center Model,” *ISACA J.*, vol. 3, 2015.

[252] Merriam-Webster, “Model,” 2016. [Online]. Available: http://www.merriam-

webster.com/dictionary/model. [Accessed: 29-Jan-2016].

[253] SEBoK, “Representing Systems with Models,” 2016. [Online]. Available: sebokwiki.org/wiki/Representing_Systems_with_Models. [Accessed: 07-Oct-2016].

[254] Wikipedia, “Operating model,” 2016. [Online]. Available: https://en.wikipedia.org/wiki/Operating_model. [Accessed: 29-Sep-2016].

[255] S. Teoh, “Journal of Information Technology Management COMPETENCY AND CAPABILITY DEVELOPMENT PROCESS: AN SME ENTERPRISE SYSTEM UPGRADE AND IMPLEMENTATION,” *Competency Capab. Process J. Inf. Technol. Manag.*, vol. XXI, no. 3, 2010.

[256] L.D. Erasmus; N du Plooy; M. Schnetler & S. Yadavalli, “Engineering Logistics of Personnel and Computer Resources of a Command and Control Centre: Desk Study (PDF Download Available),” 2015. [Online]. Available: https://www.researchgate.net/publication/281967982_Engineering_Logistics_of_Personnel_and_Computer_Resources_of_a_Command_and_Control_Centre_Desk_Study. [Accessed: 20-Mar-2018].

[257] R. Oosthuizen and J. H. Roodt, “Credible Defence Capability: Command and Control at the Core,” *L. Warf. Conf.*, 2008.

[258] Brigadier-General C. Gildenhuys, “Armour…Combat Arm of Decision,” 2013. .

[259] C. Kerr; R. Phaal & D. Probert, “A framework for strategic military capabilities in defense transformation,” in *11th International Command and Control Research and Technology Symposium ‘Coalition Command and Control in the Networked Era,’* 2003.

[260] M. Lizotte; F. Bernier; M. Mokhtari; M. Couture; G. Dussault; C. Lalancette & F. Lemieux, “Towards a Capability Engineering Process,” 2004. [Online]. Available: http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA432358. [Accessed: 29-Sep-2016].

[261] G. White, “Capability Based Planning… and Grass,” 2013. [Online]. Available: http://enterprisearchitects.com/capability-based-planning-and-grass/. [Accessed: 29-Sep-2016].

[262] eWorks Moodle, “Content Development Demo,” 2016. [Online]. Available: https://moodle.eworks.edu.au/mod/book/view.php?id=6988. [Accessed: 23-Jan-2017].

[263] ITILnews.com, “ITIL Back to basics (People, Process and Technology),” 2015. [Online]. Available: http://www.itilnews.com/ITIL__Back_to_basics_People_Process_and_Technology.html. [Accessed: 26-Nov-2018].

[264] G.J. Botha & M. de Vries, “Towards a Capability Planning / Design Methodology for Enterprises Handling Anthropogenic Hazards,” 2012. [Online]. Available: http://conferences.sun.ac.za/index.php/cie/cie-42/paper/view/67/33. [Accessed: 29-Sep-2016].

[265] NIST, “National Cybersecurity Workforce Framework,” 2013. [Online]. Available: http://csrc.nist.gov/nice/framework/. [Accessed: 17-Feb-2016].

[266] Department of Labour, “Basic Conditions of Employment Amendment Act No 11 of 2002,” 2002. [Online]. Available: http://www.labour.gov.za/DOL/downloads/legislation/acts/basic-conditions-of-employment/Amended Act - Basic Conditions of Employment.pdf. [Accessed: 03-Oct-2016].

[267] J de Waal, “Understanding the Complexity of Systems by Using the Concept Interface Matrix (CIM).,” 2013. [Online]. Available: http://incose.org.za/pubs/2013/incosesa2013_submission_3.pdf. [Accessed: 03-Oct-2016].

[268] V. Naido, “Police Service on launch of minimum physical security standards,” 2009. [Online]. Available: http://www.gov.za/police-service-launch-minimum-physical-security-standards. [Accessed: 03-Oct-2016].

[269] J. Thaba & S. Benade, “Aligning Force Planning and Systems Acquisition,” 2015. [Online]. Available: www.iamot2015.com/2015proceedings/documents/P009.pdf. [Accessed: 03-Oct-2016].

[270] National Treasury, “Public Finance Management Act,” 2012. [Online]. Available: www.treasury.gov.za/legislation/pfma/act.pdf. [Accessed: 03-Oct-2016].

[271] Wikipedia, “Operating Model,” 2017. [Online]. Available: https://en.wikipedia.org/wiki/Operating_model. [Accessed: 22-Mar-2017].

[272] D. Cooper; S. Dhiri & J. Root, “Winning operating models,” 2012. [Online]. Available: http://www.bain.com/Images/BAIN_BRIEF_Winning_operating_models.pdf. [Accessed: 04-Oct-2016].

[273] J. Ross; P. Weill; D.C. Robertson, *Book Review: Enterprise Architecture As Strategy: Creating a Foundation for Business Execution.*, vol. 25, no. 4. Harvard Business Review Press, 2008.

[274] D. Williams & J. Leask, “People, Process, Technology Strategy for Enterprise 2.0,” 2011. [Online]. Available: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0ahUKEwjPr4iWqLTPAhULL8AKHQUHB1MQFgghMAE&url=https%3A%2F%2Fwww.boozallen.com%2Fcontent%2Fdam%2Fboozallen%2Fmedia%2Ffile%2FPeople-Process-Technology-Enterprise2.pdf&usg=AFQjCNFdrhPB1RvrDFZ. [Accessed: 29-Sep-2016].

[275] M. De Vries, A. Van Der Merwe, P. Kotzé, and A. Gerber, “A method for identifying process reuse opportunities to enhance the operating model,” in *IEEE International Conference on Industrial Engineering and Engineering Management*, 2011, pp. 1005–1009.

[276] Cisco Systems, “Introduction to eTOM,” 2009. [Online]. Available: http://www.cisco.com/c/en/us/products/collateral/services/high-availability/white_paper_c11-541448.html. [Accessed: 26-Nov-2018].

[277] Wikipedia, “TM Forum,” 2016. [Online]. Available: https://en.wikipedia.org/wiki/TM_Forum. [Accessed: 05-Oct-2016].

[278] IBM, “Insurance Application Architecture (IAA),” 2009. [Online]. Available: http://www.ibm.com/support/knowledgecenter/SSAVUV_7.0.0/com.ibm.ws.icp.insp_cfep1.doc/ins/pc/p_cdev/concept/ci/indstds/c_iaa.html. [Accessed: 04-Oct-2016].

[279] BIAN, “Banking Industry Architecture Network,” 2016. [Online]. Available: https://bian.org/. [Accessed: 04-Oct-2016].

[280] IBM, “Information Framework (IFW),” 2009. [Online]. Available: http://www.ibm.com/support/knowledgecenter/SSQH9M_7.0.0/com.ibm.ws.icp.bkkpayfep1.doc/bkk/pay/paymdev/concept/ci/indstds/c_ifw.html. [Accessed: 04-Oct-2016].

[281] S. Spafford, G., Wheeler, A. J. & Mingay, “Updates in COBIT 5 Aim for Greater Relevance to Wider Business Audience.,” 2012. [Online]. Available: https://www.gartner.com/doc/1982323. [Accessed: 26-Nov-2018].

[282] S. Claes, “Next Generation IT operating models - KPMG,” 2014. [Online]. Available: http://www.kpmg.com/BE/en/IssuesAndInsights/ArticlesPublications/Documents/Next-Generation-IT-

Delivery-Models.pdf. [Accessed: 05-Jan-2016].

[283] P. Ditrans; A. Anand; M. Ponnuveetil; A. Acharya & S. Dash, “Why New-age IT Operating Models are Necessary for Enhanced Operational Agility,” 2016. [Online]. Available: https://www.cognizant.com/whitepapers/why-new-age-it-operating-models-are-necessary-for-enhanced-operational-agility-codex1399.pdf. [Accessed: 05-Oct-2016].

[284] TMForum, “Business Process Framework,” 2013. [Online]. Available: https://www.tmforum.org/business-process-framework/. [Accessed: 26-Nov-2018].

[285] H. Jiejin, “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, 2009.

[286] J.E. Cartwright, “Joint Terminology for Cyberspace Operations,” 2014. [Online]. Available: www.nsci-va.org/CyberReferenceLib/2010-11-joint Terminology for Cyberspace Operations.pdf. [Accessed: 10-Feb-2016].

[287] D. Milham, “How can the eTOM Framework help Service Providers in today’s market place?,” *Netw. Oper. Manag. Symp.*, vol. Volume 2, pp. 59–71, 2004.

[288] TM Forum, “Application Framework (TAM),” 2016. [Online]. Available: https://www.tmforum.org/application-framework/. [Accessed: 05-Oct-2016].

[289] TM Forum, “Information Framework (SID),” 2016. [Online]. Available: https://www.tmforum.org/information-framework-sid/. [Accessed: 05-Oct-2016].

[290] TM Forum, “Integration Framework,” 2016. [Online]. Available: https://www.tmforum.org/integration-framework/. [Accessed: 05-Oct-2016].

[291] wiseGEEK, “What is ETOM?,” 2013. [Online]. Available: http://www.wisegeek.com/what-is-etom.htm.

[292] APMG International, “What is a Maturity Model, and why use one?,” 2016. [Online]. Available: http://www.apmg-international.com/en/consulting/what-maturity-model.aspx. [Accessed: 06-Oct-2016].

[293] T. Mettler, “Maturity assessment models: a design science research approach,” *Int. J. Soc. Syst. Sci.*, vol. 3, no. 1/2, pp. 81–98, 2011.

[294] Office of Electricity Delivery and Energy Reliability, “Cybersecurity Capability Maturity Model (C2M2).” [Online]. Available: http://energy.gov/oe/services/cybersecurity/cybersecurity-capability-maturity-model-c2m2-program. [Accessed: 06-Oct-2016].

[295] J. Becker, R. Knackstedt, and J. Pöppelbuß, “Developing Maturity Models for IT Management,” *Bus. Inf. Syst. Eng.*, vol. 1, no. 3, pp. 213–222, 2009.

[296] G. Lahrmann, F. Marx, T. Mettler, R. Winter, and F. Wortmann, “Inductive design of maturity models: Applying the Rasch algorithm for design science research,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 6629 LNCS, pp. 176–191, 2011.

[297] BSIMM, “Building Security In Maturity Model,” 2016. [Online]. Available: https://www.bsimm.com/. [Accessed: 06-Oct-2016].

[298] K. Ferraiolo, “Systems Security Engineering – Capability Maturity Mode,” 2016. [Online]. Available: http://csrc.nist.gov/nissc/2000/proceedings/papers/916slide.pdf. [Accessed: 26-Nov-2018].

[299] OWASP, “Software Assurance Maturity Model (openSAMM),” 2016. [Online]. Available:

http://www.opensamm.org/. [Accessed: 06-Oct-2016].

[300] R. Pereira and M. M. Da Silva, “A maturity model for implementing ITIL V3 in practice,” *Proc. - IEEE Int. Enterp. Distrib. Object Comput. Work. EDOC*, pp. 259–268, 2011.

[301] A. Pederiva, “The COBIT Maturity Model in a Vendor Evaluation Case,” *Inf. Syst. Control J.*, vol. 3, no. 26–29, 2003.

[302] A. Pasquini and E. Galiè, “COBIT 5 and the Process Capability Model. Improvements Provided for IT Governance Process,” *Proceedings of FIKUSZ ’13 Symposium for Young Researchers*, 2013. [Online]. Available: https://kgk.uni-obuda.hu/sites/default/files/06_Pasquini_Galie.pdf. [Accessed: 12-Jun-2018].

[303] I. MacDonald, “ITIL Process Assessment Framework,” 2010. [Online]. Available: http://www.itsmfi.org/files/ITIL Process Assessment Framework - MacDonald.pdf.

[304] Wikipedia, “ISO/IEC 21827,” 2016. [Online]. Available: https://en.wikipedia.org/wiki/ISO/IEC_21827. [Accessed: 06-Oct-2016].

[305] International Standards Organisation, “ISO/IEC 21827:2008 Information technology -- Security techniques -- Systems Security Engineering -- Capability Maturity Model® (SSE-CMM®),” 2016. [Online]. Available: http://www.iso.org/iso/catalogue_detail.htm?csnumber=44716. [Accessed: 06-Oct-2016].

[306] ITU-T, “ITU T X.1055 Risk management and risk profile guidelines for telecommunication organizations.” [Online]. Available: https://www.itu.int/rec/T-REC-X.1055-200811-I. [Accessed: 26-Nov-2018].

[307] ISO/IEC, “Introduction To ISO 27011 (ISO27011),” 2008. [Online]. Available: http://www.27000.org/iso-27011.htm. [Accessed: 26-Nov-2018].

[308] ISO/IEC, “ISO/IEC 27005 risk management standard,” 2011. [Online]. Available: http://www.iso27001security.com/html/27005.html. [Accessed: 11-Dec-2017].

[309] The Open Group, “FAIR–ISO/IEC 27005 Cookbook,” 2010. [Online]. Available: http://www.businessofsecurity.com/docs/FAIR - ISO_IEC_27005 Cookbook.pdf. [Accessed: 26-Nov-2018].

[310] D. Kosutic, “ISO 31000 and ISO 27001 – How are they related?,” 2014. [Online]. Available: https://advisera.com/27001academy/blog/2014/03/31/iso-31000-and-iso-27001-how-are-they-related/. [Accessed: 11-Dec-2017].

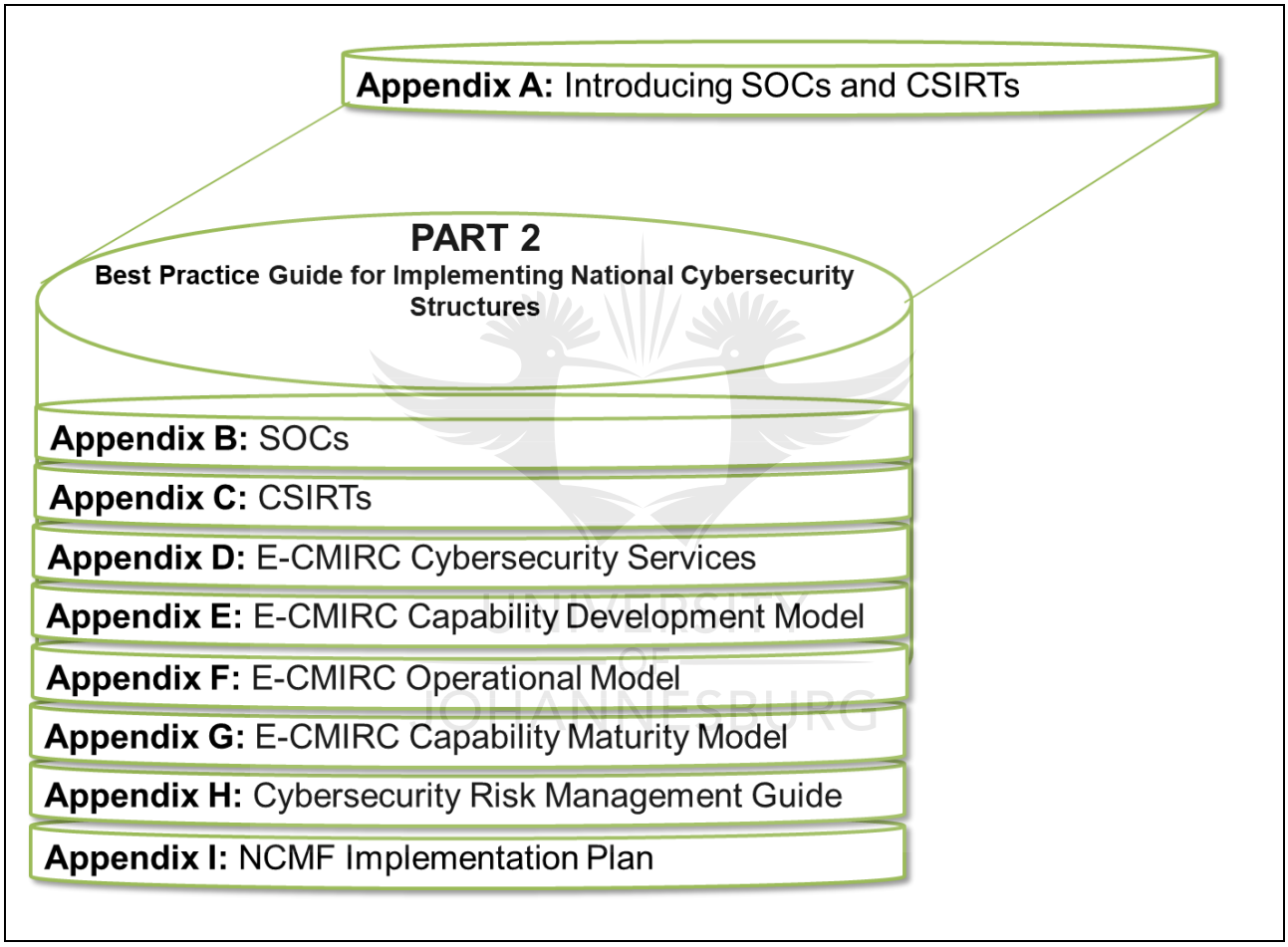
[311] Boundless, “Strategic, Tactical, and Operational Control,” *Boundless Management*, 2015. [Online]. Available: https://www.boundless.com/management/textbooks/boundless-management-textbook/control-8/types-of-control-62/strategic-tactical-and-operational-control-313-3960/. [Accessed: 29-Feb-2016].

[312] D. Black, “Accountability vs. Responsibility?,” 2013. [Online]. Available: http://danblackonleadership.info/archives/2921. [Accessed: 06-Jun-2018].

[313] N. Belludi, “Delegation: Accountability vs. Responsibility,” 2007. [Online]. Available: http://www.rightattitudes.com/2007/08/13/delegation-accountability-responsibility/. [Accessed: 06-Jun-2018].

# PART 2

## Best Practice Guide for the Implementation of National Cybersecurity Structures


Appendix A: Introducing SOCs and CSIRTs
PART 2
Best Practice Guide for Implementing National Cybersecurity Structures
Appendix B: SOCs
Appendix C: CSIRTs
Appendix D: E-CMIRC Cybersecurity Services
Appendix E: E-CMIRC Capability Development Model
Appendix F: E-CMIRC Operational Model
Appendix G: E-CMIRC Capability Maturity Model
Appendix H: Cybersecurity Risk Management Guide
Appendix I: NCMF Implementation Plan

# Appendix A: Introducing SOCs and CSIRTs

## A1 Introduction

In the preceding chapters, we concluded the development and illustrative application of the NCMF in context of South Africa as a developing country. We will now use Appendix A to provide a high-level, general introduction to SOCs and CSIRTs. These are the two structures from where the *monitoring and evaluation*, and *incident handling* functions are offered. A high-level overview of SOCs will be provided in Section A3, and an overview of CSIRTs will be provided in Section A4. This will provide the reader with a basic understanding of these structures, and this understanding will help with the orientation and interpretation of the discussion of their functions in the chapters following.

As stated in Chapter 2, cybersecurity functions and its services are offered from different structures. It is important for us to identify the structures from where the *monitoring and evaluation* function, and *incident handling* functions are offered from, as this allows us to identify its services. Before we start with a discussion on the structures, we will reinforce our motivation for the selection of the *monitoring and evaluation* function, and the *incident handling* functions in Chapter 4. These two functions' corresponding structures are SOCs and CSIRTs. Appendix A is structured as follows:

**Section A2** motivates our selection of the *monitoring and evaluation*, and *incident handling* function. It is necessary to strengthen the understanding of our selection since their complementary structures will be used to identify services and technologies for the E-CMIRC.

**Section A3** introduces the SOC structure at a high level.

**Section A4** introduces the CSIRT structure at a high level.

**Section A5** concludes Appendix A, and provides two ways of viewing the Monitor and Evaluate and Incident Handling function.

## A2 Motivation for functions selected for E-CMIRC structure

In Chapter 4, South African authoritative sources were identified to assist with the identification of its national cybersecurity functions. International normative sources were also identified, and analysed, to

identify thirteen of the most general functions. The general cybersecurity functions we have identified using South African authoritative, and international normative sources, were then correlated to, and verified and validated against a random, and blind selection of international authoritative sources.

The dimensions, mandates and domains the NCMF operate in, were introduced in Chapter 3. The dimensions, mandates and domains introduced in Section 3.5 to Section 3.8, together with the National Strategic Risk and Threat Assessment Guide introduced in Appendix H, assist with the selection and prioritisation of one, or many of the cybersecurity functions for implementation at national level.

There is an overlap in some of the services and technologies of some of the national cybersecurity functions, such as the services and technologies of the *monitoring and evaluation*, and the *incident handling* functions. This overlap in services and technologies means that developing countries can realise a cost saving by identifying these overlapping services and technologies, and offering them from a single, national structure.

In this regard, it can be noted that*the monitoring and evaluation*, and the *incident handling* functions have a common service, the incident management service. This common service could use the same technology and processes. Using the same technology and processes has the advantage in that money is spent on only one technology, and only one set of skills is needed to support this technology.

The two cybersecurity functions' overlapping services and technologies will be identified and offered from a newly envisioned cybersecurity structure. Our new structure is called the E-CMIRC. The development of the E-CMIRC models will allow us to illustrate the application of the NCMF implementation part (levels 4 to 6).

Our selection was made based on our experience in planning, building, running and monitoring these two cybersecurity functions and its structures, both at national and organisational level, as well as the fact that their needed skillsets, services and technologies overlap. Another reason for selecting these two functions with their complementary structures for the development of the E-CMIRC, is that there are a large number of reference implementation architectures for both. Most developed nations have a national CSIRT structure offering the services to realise the *incident handling* function, and there exists abundant reference material in terms of its services. The same holds true for the *monitoring and evaluation* function whose services are offered from a SOC structure. There is ample reference material on how to plan, build, run and monitor CSIRTs and SOCs. We will now provide a high-level introduction to the SOC structure.

## A3 Introduction to the SOC structure

As part of a defence in depth strategy [71] [132], organisations and nations deploy technical controls to mitigate risks associated with the cyber environment. Some examples of these technical controls are network-based

controls to protect the network itself (such as firewalls, intrusion protection systems and network access control), network-based controls to protect information (data loss prevention), or host-based controls (anti-malware, file integrity monitoring). These controls need to be monitored to ensure that they work as intended, and to detect attacks against the organization. To achieve this objective, and depending on the monitoring and log collection deployment model, the logs of the technical controls are collected, correlated, and in some instances aggregated, and then forwarded to a SOC. From the events in the logs, detected anomalies and attacks results in incidents, and these incidents need to be handled, either by the SOC itself, or by a CSIRT.

There is currently an increase in the establishment of SOCs and CSIRTs due to the drive by governments and industry to address the ever increasing cyber threat [133]. Other driving factors are the requirements expressed in authoritative sources (NCSs, acts and regulations) as discussed in Chapter 3, and requirements, expressed by various normative sources, such as standards and best practices. Some of the normative sources expressing monitoring requirements are:

- COBIT 4.1 - DS5.5 Security testing, surveillance and monitoring [134].
- IITIL v3 - SO 5.13 Information security management and service operation [135].
- ISO/IEC 27002:2005 - 10.10.2 Monitoring system use, 10.10.3 Protection of log information, 10.10.4 Administrator and operator logs, 15.3.1 Information systems audit controls [135].
- SANS critical controls - critical control 14: maintenance, monitoring, and analysis of security audit logs [51].
- NIST SP 800-53 - 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) [136].



In addition to the normative and authoritative requirements for ICT monitoring, there are also tangible business benefits to be gained, which further drives the need for monitoring. Key to this, is that monitoring fulfils a portion of the risk management strategy for services and infrastructure, and it precipitates in the following benefits that are equally applicable to nation states [137]. In addition to there being a lower interruption of critical services, critical infrastructure and business processes, monitoring.

- Lower interruption to critical services, critical infrastructure and business processes.
- Transforms a business or nation from a reactionary posture to a prepared posture.
- Controls and prevents threats.
- Releases critical IT and network resources.
- Preserves accountability and corporate governance.
- Provides and maintains privacy for the public, employees, partners and customers.
- Produces a situational awareness.

Taking into consideration the definitions and description of SOCs, we can conclude that SOCs thus serve as a central repository for logs that are scanned to detect anomalies, and to identify possible attacks against an organisation or nation. Typical functions offered by SOCs are monitoring, incident management and the mitigation and containment of threats detected against assets. To this effect, a well-functioning SOC can mitigate some of the cyber risks to which nations or organisations are exposed. SOC functions are discussed in more detail in Appendix B.

There is currently no publicly available standard for building SOCs [138], but there are numerous frameworks and best practices that could be applied to SOCs in terms of operational management. Some examples are ITIL [139] for operations management, and ISO/IEC 27001:2013 [48] for cybersecurity management. From the SOC definitions, we have seen that one of the key services of a SOC, is incident management. In keeping with our intention of identifying functions with overlapping services and technologies, we will now introduce the CSIRT structure, whose primary function is one of incident management.

## A4: Introduction to the CSIRT Structure

The abbreviation, CSIRT stands for a computer security incident response team. The abbreviation is mostly used in Europe for the protected Computer Emergency Response Team (CERT), or Computer Emergency Response Team Coordination Centre (CERT-CC) name. The names “CERT” and “CERT/CC” are registered and owned by the Software Engineering Institute (SEI) at the Carnegie Mellon University (CMU). The CMU CERT was the first CSIRT [140]; [141].



The CERT/CC forms a sub-component of the larger CERT division. CERT is a name, and not an acronym [141]. Many CSIRTs have been allowed by CMU to use the name CERT or CERT/CC in their names, but these are independent of the university. Many of these CSIRTs are however members of the Forum of Incident Response and Security Teams (FIRST) community, of which the CERT/CC was a founding member. For the purpose of developing the E-CMIRC model, and for reference to an incident resolution capability, we will use the acronym CSIRT.

It is further our experience that most often, a structure’s function may be derived from its definition and description. We will now introduce some of the CSIRT definitions from literature sources. The OAS [126] defines a national CSIRT as an entity that serves a defined community, and coordinates incidents at a national level. It further serves as a contact point for national and international incidents.

The European Agency for Network and Information Security (ENISA) defines a CSIRT as “*a team of IT security experts whose main business is to respond to computer security incidents. It provides the necessary services*

*to handle them and support their constituents to recover from breaches"* [140], while Ruefle [142], defines a CSIRT as:

> *"…a concrete organizational entity (that is, one or more staff) that is assigned the responsibility for coordinating and supporting the response to a computer security event or incident. CSIRTs can be created for nation states or economies, governments, commercial organizations, educational institutions, and even non-profit entities. The goal of a CSIRT is to minimize and control the damage resulting from incidents, provide effective guidance for response and recovery activities, and work to prevent future incidents from happening."*

The Software Engineering Institute (SEI) [81] at the Carnegie Mellon University defines a CSIRT as:

> *"…a service organisation that is responsible for receiving, reviewing, and responding to computer security incident reports and activity. Their services are usually performed for a defined constituency that could be a parent entity such as a corporate, governmental, or educational organization; a region or country; a research network; or a paid client."*

Taking into consideration the formal definition of CSIRTs, it can be concluded that the main function of a CSIRT is to perform incident handling.

The Computer Emergency Response Team (CERT) [143] states that the function or roles of CSIRTs are to receive, review and respond to cybersecurity incident reports and activity. CSIRTs are service oriented organisations [141]. Incident Handling services are reactive in nature. The purpose of a CSIRT is "to "minimize the impact of an incident to a company, and allow it to get back to work as quickly as possible" [144], or "to serve as a focal point in the prevention, receiving and responding to computer security incidents" [126] [145].



CSIRTs are made up of teams responding to cybersecurity incidents. The terms CSIRT is used as a generic description of an incident response team [146], while CERT is a trademarked name which is controlled by CERT/CC [147] as explained in Appendix A. In the development of the E-CMIRC model, we will be using the term "CSIRT." There are different CSIRT structures, types and service delivery models, and all of them are discussed to determine the model best suited for the E-CMIRC. Our intention with this Appendix is further to identify CSIRT functions. The most relevant and applicable functions and service delivery models from the SOC and CSIRT structures will then be identified, and motivated, and combined in Appendix D to compile a list of functions for the E-CMIRC.

ENISA defines a CSIRT as "*a* team of IT security experts whose main business is to respond to computer security incidents. It provides the necessary services to handle them and support their constituents to recover from breaches" [148]. National CSIRTs should build relations with national and international structures and stakeholders to foster collaboration and cooperation across borders.

These functions and roles are confirmed by Morgus; Skierka; Hohmann and Mauer [149]. Morgus *et al* describes a national CSIRT as an entity acting as the primary national interface between domestic incident responders (in a South African context, these would be sector-CSIRTs), as well as other national CSIRTs globally. A national CSIRT, subject to the country's political and legal setting, could also be used to provide additional functions, such as forensic and awareness functions.

The Software Engineering Institute (SEI) at the Carnegie Mellon University (CMU) defines a national CSIRT as a structure that coordinates incident management at national level, and promotes the comprehension of cybersecurity related matters for the national community [150]. This includes awareness programmes. A national CSIRT should further be able to provide technical competence in the resolution of national cybersecurity incidents, and to disseminate this information to its constituents.

ENISA defines a government CSIRT as "*… governmental CSIRTs are typically used to protect the cyberspace of governmental institutions including critical infrastructure as well as to ensure cyber-crisis management.*" [151], while Ruefle [152] defines a government CSIRT as "…may be involved in security awareness training and general incident handling activities but never perform any forensics activities." Just as the SOC as an entity has its own SOC specific functions (Section A3), so does a CSIRT. The CSIRT, as a structure, offers the CSIRT structure functions to realise the incident handling function.

Driving factors for the establishment of CSIRTs are the requirements expressed in authoritative sources (NCSs, acts and regulations) as discussed in Chapter 3) Incident handling is also expressed as a requirement by various normative sources such as:

- COBIT 4.1 - DS5.6 Security incident definition, DS8.3 Incident escalation, DS8.4 Incident closure [134].
- ITIL v3 - SD 4.5.6.2 Management of security breaches and incidents, SO 4.1 Event management, ST, SO 4.2 Incident management [135].
- ISO/IEC 27002:2005 - 13.0. Information security incident management; 13.2. Management of information security incidents and improvements; 13.2.2. Learning from information security incidents [135].
- SANS Critical Controls - CSC 19: Incident response and management [51].
- NIST SP 800-53 - IR 1-7 Incident response [136].

During our introduction and description of functions, services, capabilities and structures in Chapter 2 we explained that functions consists of services, and services consists of capabilities which are made up of people, processes and technologies. One of the services that makes up the *Incident Handling* function, is the incident management service. Therefore, while the main function of a SOC is to provide the *monitoring and evaluation* function, one of its services is an incident management service. The CSIRTs main function is the Incident Handling function, which also consists of an incident management service.

One way of looking at the two selected functions – the *monitor and evaluate* function, and the *incident handling* function, is that the events, threat intelligence and other security related information collected by SOCs (SOC services), could serve as input to the CSIRT. From this point of view, the *monitor and evaluate* function serve to enhance the CSIRT *incident handling* function. Augmenting the CSIRT services with SOC services allows CSIRTs to provide early warning, and remediation information to its constituents. In this instance, the *incident handling* function is seen as the primary function and is supported by SOC's *monitor and evaluate* function.

Another way of looking at the *incident handling* function in context of SOCs and CSIRTs, is that a CSIRT's *incident handling* function could be viewed as a highly specialised, highly mature, sub-function of the SOC's inherent *incident handling* function. For example, Standard Bank, a commercial bank in South Africa [153] has a highly effective SOC, and only in the event of cybersecurity events being detected, and classified as incidents, do they invoke a virtual-CSIRT to handle the incidents – such as when the theft of R300 million in 2016 occurred in a scam originating from Japan [154]. In this instance, the *monitor and evaluate* function is seen as the primary function and is supported by the *incident handling* function.

## A5 Conclusion

SOCs primarily provide a *monitoring and evaluation* function with secondary incident management services to organisations or government departments, while CSIRTs primarily offer an *incident handling* function that consists of incident management services, at organisational and national level. The fact that both SOCs and CSIRTs inherently deliver an incident management service necessitates the need to further explore the two structure's similarities and differences in terms of services and technologies.



This will allow us to identify services and technologies different, but also similar to both structures. We will be doing this since our intention is to realise cost and skills saving by combining and offering their overlapping services and technologies in terms of the E-CMIRC structure.

Based on our experience working on cybersecurity projects at national level, combined with our experience in enterprise architecture, tangible benefits are gained by combining the services and technologies of two or more cybersecurity functions. Some of the key benefits gained by combining the services and technologies of two or more functions are:

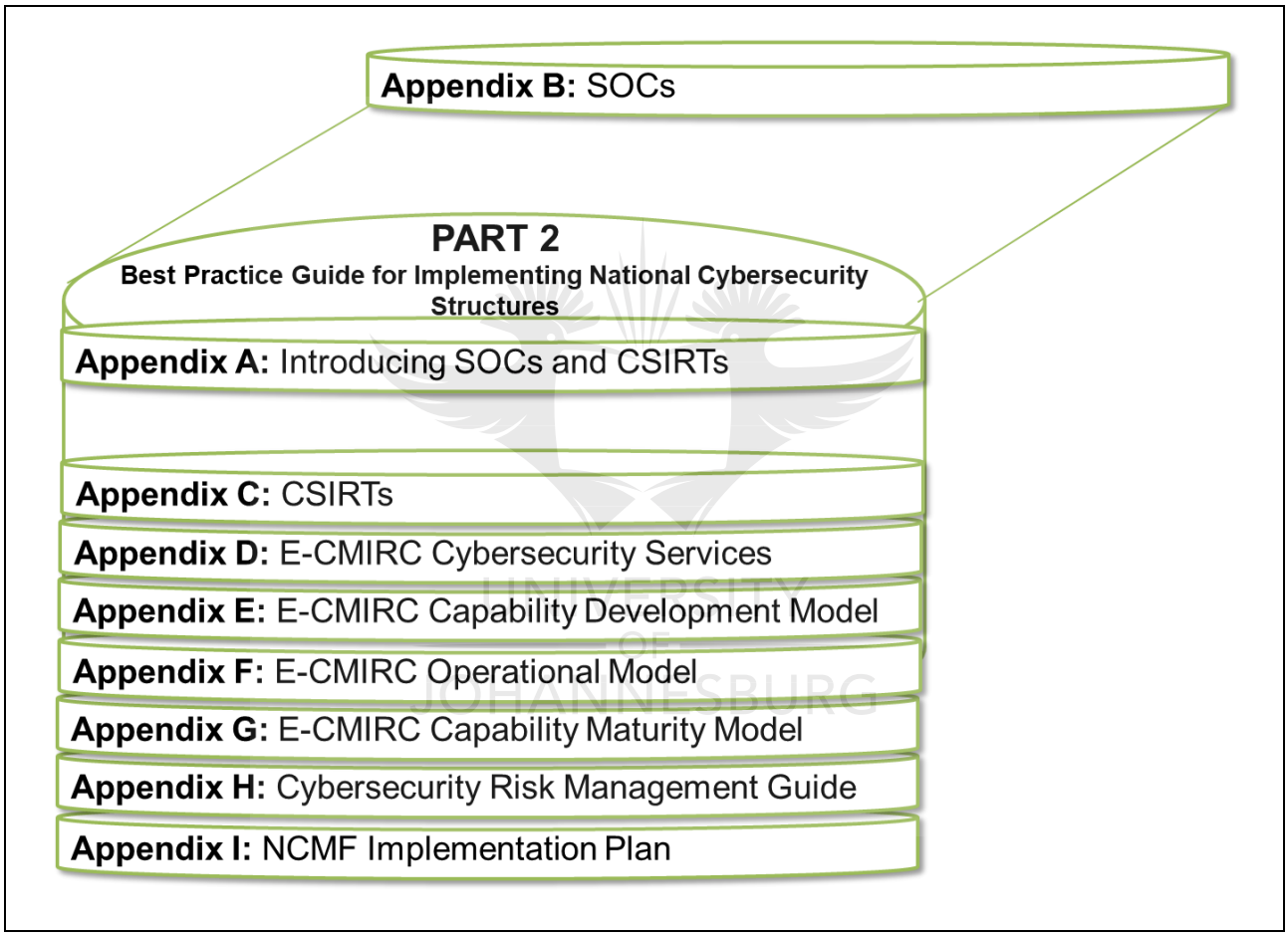
- Cost saving may be achieved through the combination and alignment of the service's processes.For example, the incident management processes for SOCs and CSIRTs may be combined into one incident management process addressing the similarly named incident management service. This single incident management process also has to integrate and align with the state's escalation process and media handling process. Generally speaking, aligning processes across different government departments may

realise a cost benefit. It may also lead to process automation leading to the correct and timeous execution of processes, and in some cases, negates the need for human intervention.

- Offering two or more national cybersecurity functions from a single structure offers a savings in terms of shared infrastructure, such as facilities, connectivity, equipment and other resources.
- Using one technology system to realise more than one cybersecurity service, also leads to a cost reduction and saving. For example, both SOCs and CSIRTs offer the incident management service. The technology used by SOCs is a SIEM, and this is unique to a SOC. Most modern SIEMs also provide incident management software and integration as part of the SIEM capability suite. This SIEM technology may be used to realise the incident management services of both SOCs and SIEMs, eliminating the need for separate technologies, while providing additional services such as log collection, aggregation and correlation.
- Fewer technological systems reduces the need for multiple technology experts and skills. This has a cost benefit in that fewer human resources are needed to support the technologies. It also allows the people component to focus on process management and service tasks.

Now that we have done a high-level introduction of SOCs and CSIRTs, the SOC functions and service delivery models are introduced and discussed in Appendix B and the CSIRT functions and service delivery models are introduced in Appendix C. Our motivation for the discussion on the service delivery models is that different service delivery models need different functions and services.

We will then be identifying SOC and CSIRT overlapping services and technologies in Appendix D. Identifying SOC and CSIRT overlapping services and technologies are crucial since we will be combining them and offer them from our E-CMIRC. The E-CMIRC is a national structure that will offer overlapping SOC and CSIRT services, while consolidating the technology and processes needed to enable those services, at the same time


Appendix B: SOCs
PART 2
Best Practice Guide for Implementing National Cybersecurity Structures
Appendix A: Introducing SOCs and CSIRTs
Appendix C: CSIRTs
Appendix D: E-CMIRC Cybersecurity Services
Appendix E: E-CMIRC Capability Development Model
Appendix F: E-CMIRC Operational Model
Appendix G: E-CMIRC Capability Maturity Model
Appendix H: Cybersecurity Risk Management Guide
Appendix I: NCMF Implementation Plan

# Appendix B: SOCs

## B1 Introduction

We introduced SOCs in Appendix A. This was an extremely high-level introduction, and we touched on some of its functions. In this appendix, we will provide a more detailed discussion on the SOC structure, and we will use this appendix further to identify the SOC functions, as well as its service delivery models. Some of the key components of an IT service delivery model are the governance of E-CMIRC services, organisation of E-CMIRC services, E-CMIRC operational processes, and performance management [155].

We explained in Chapter 4 and Appendix A that a cost and skills saving may be realised if the technologies and processes of two, or more cybersecurity functions are combined and offered from a single structure. This alignment of technology and processes, makes it necessary for us to identify different service delivery models. Different service delivery models offer different services, using different technologies and processes.

IT Services may be offered "as a service," or by “augmenting staff” [156]. Various permutations of these two models exist. Service delivery realises benefits, and deliver on functions. There are publicly available service delivery frameworks that may be used as a reference. An example of a service delivery framework, is ITIL's IT Service Management (ITSM) [157]. Selecting the right service delivery model for the E-CMIRC realises the following benefits [155]:

- It aligns services and technology.
- It allows for business processes to be aligned
- Cost efficiency is realised.
- Agile response to change in the business environment.



We have illustrated that we can use the general cybersecurity functions, as well as the domain lifecycle phases to identify cybersecurity structures, and we identified SOCs in Section 4.6.8 as the structures providing the *monitoring and evaluate* function, and CSIRTs in Section 4.6.7 as the structure providing the *incident handling* function. We will in this appendix introduce SOC structures, its service delivery models and functions. From these functions, we will make a selection for our E-CMIRC.

The rest of the chapter is structured as follows:

**Section B2** introduces the SOC structures and service delivery models. SOCs may be structured to offer internally focussed services to a single entity or organisation, or externally to multiple entities or organisations.

**Section B3** identifies the SOC primary functions to be used during the development of the E-CMIRC.

**Section B4** identifies and motivates the most suitable SOC service delivery model for use by the E-CMIRC.

## B2 SOC structures and service delivery models

Our intention is to use this appendix to identify SOC functions, as well as the SOC service delivery models, and select functions and a service delivery model for the E-CMIRC. It should be understood the SOC and CSIRT functions are different to the national cybersecurity functions or general cybersecurity functions. The SOC and CSIRT functions are structure specific, in other words, specific to the SOC and CSIRT structures, and consist of their function's specific services. Structural cybersecurity functions should not be confused with national cybersecurity functions. The two types of security functions we are discussing in this thesis are:

- The general cybersecurity functions that we identified in Chapter 4.
- The cybersecurity structure's specific functions. These we will identify in Appendices B and C respectively.

Our approach to identifying the two different functions and services is shown in Figure 34.

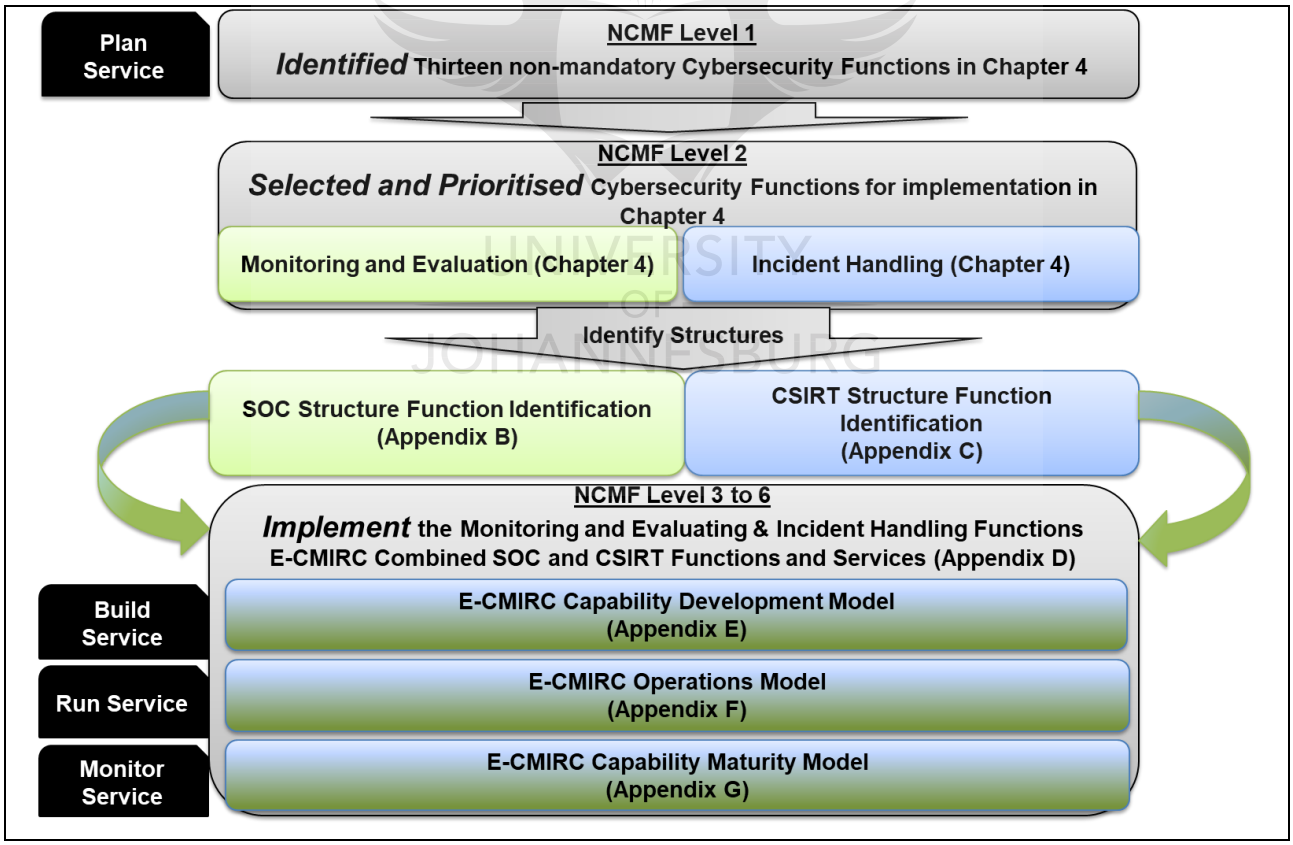



**Figure 34: E-CMIRC Development Approach**

Figure 34 shows that NCMF levels 1 to 2 were used to identify thirteen general and non-mandatory cybersecurity functions. This was done in Chapter 4. We then selected and motivated two functions in Chapter 4, for the development of the E-CMIRC structure. The two selected functions are the *monitoring and evaluate* function, and the *incident handling* function.

To prepare for the implementation of these functions using the E-CMIRC structure, we will introduce and discuss the *monitoring and evaluation* function's structure, the SOC, in Appendix B and the *incident handling* function's structure, the CSIRT, in Appendix C. These two structures' functions are determined, overlaps identified, and we will then correlate the overlapping functions to identify E-CMIRC functions.

The SOC and CSIRT structure's services with similar processes and technologies are identified, and combined in Appendix D (as indicated by the two arrows), and these services are then offered by the E-CMIRC. The NCMF level 3 to level 6 is then applied to implement the E-CMIRC. The NCMF satisfies the plan function, while the E-CMIRC descriptive models satisfies the build, run and monitor functions of the PBMR organisational framework.

We need to identify the structure's functions first before we can discover its services. This flows from our discussion on functions, services, capabilities and structures in Chapter 2 where we have explained that functions are made up of services. With the identification, selection and prioritisation tasks now concluded, we will start with our preparation for the implementation part of the *monitoring and evaluation,* and *incident handling*, functions. We will do this by analysing SOC and CSIRT structures, and identify its overlapping functions, services and technologies in Appendix B and Appendix C, and propose services for the E-CMIRC in Appendix D.



The *Monitor and Evaluate* function is offered from a SOC [158] [159] [160]. A SOC is an organised structure consisting of highly skilled people. The mission of a SOC is to monitor and advance the organisational or national cybersecurity posture.

SOCs use SIEM tools to prevent, detect, analyse and respond to cybersecurity incidents [161]. SIEM technology components typically consists of a log manager, correlation engine, automated workflow, incident management and reporting engine to name a few [162] [163]. SOCs are extremely expensive to build and run, and as such, some service providers offer SOCs as a service. These are typically referred to as managed security service providers (MSSPs) [164] [165]. MSSPs is an example of an external SOC structure residing outside organisational boundaries.

It is our experience that SOC services are used mostly by organisations or single government departments, and government structures. While it is not common to find SOC structures at national level, there are a few examples of SOCs being utilised at national level. Such an example is the Korean Internet and

Security Agency (KISA) in South Korea [166]. SOC structures can be localised, or geographically dispersed [167].

From a South African perspective, the intention of the State Information Technology Agency (SITA) 2012 was to build a SOC to monitor their government clients [168]. In some instances, the departments of defence of some nations build SOCs in order to provide a network-centric warfare capability, as well as a defensive and offensive capability, but these structures most often only have military applications. Some nations with military SOCs are Australia, China, India, Myanmar, North and South Korea, and the United States of America [169]. The South African Department of Defence is also mandated by the NCPF to build a cyber command which would provide these capabilities [33]. Our experience has shown that SOCs can be structured as follows:

- **External SOC or MSSPs.** The SOC services are offered to, and shared across different customers. MSSPs are external to organisations. This may be a commercial entity, or the service may be shared across government departments, such as the SSA 's monitoring of some South African government departments
- **Internal SOC**. This is the organisational, government, or national SOC structure. The SOC services are offered and consumed internally by the organisation, government or nation.

Cybersecurity services offered by SOC structures are thus delivered using two distinct service delivery models. The first model is where SOC services are delivered as an outsourced, external service, using MSSPs [170]. MSSPs serve a variety of clients from different industries, or government departments [171]. MSSP's typically offer SIEM as a Service (SaaS), and depending on the SIEM technology deploys either on-site remote log collectors, or use direct log transfer to the MSSP SIEM.

The second model is where the services are delivered internally from organisational, or in-house SOCs. These SOCs can procure and deploy SIEMs on-site, or their delivery model could be SaaS. Internal or organisational SOCs focus their efforts on the organisation to whom they provide cybersecurity services and capabilities to. [172] [173]. The two service delivery models are described in Table 31.

**Table 31: SOC Cybersecurity Service and Capability Delivery Models**

| SOC Structure | Description |
|---|---|
| MSSPs (External) | This structure provides SOC services and capabilities as–a-service to organisations [164]. This model serves different customers form different industries, and even different countries. SIEM is deployed local or SaaS. |
| SOCs (Internal) | This structure serves a single (internal) customer. The structure could be centralised, or in the case of global organisations, distributed. SIEM is deployed local or SaaS. |

SOCs can be situated locally, or be geographically dispersed (global SOCs) [174]. SOCs typically work in isolation, and it is our experience that it is uncommon for information sharing to happen between SOCs and MSSPs. This is mostly due to confidentiality clauses signed with customers. This contrasts with CSIRTs where the purpose is one of openness, and to share and disseminate information through established trust relationships and channels.

## B3 SOC Functions

It must be understood that there is a difference between the national cybersecurity functions that we identified in Chapter 4, and the SOC and CSIRT structure functions. The former is applicable at national level, while the latter is structure specific, and can be viewed as sub-functions to the national cybersecurity functions. The national *monitoring and evaluation* function may be enabled by functions and services offered from a national SOC-like structure. The SOC specific functions and services must be identified so that we can do a comparison against the CSIRT function and services.

There are similarities, but also fundamental differences between the functions and services offered from SOCs and CSIRTs. The differences are mainly in the form of the processes and technologies needed for their respective services, as well as the services themselves. These differences need to be understood, as it will serve as guidance to make a selection of the cybersecurity services and technologies for the E-CMIRC.

ISACA stated that SOCs could offer all cybersecurity functions across the protect detect, respond, and recover incident handling model, and across the people, process and technology or tools framework [175]. Some of the cybersecurity functions offered by SOCs are to defend an organisation's critical assets, assist with compliance requirements and respond to cybersecurity threats in a timely fashion [176].



These functions are enabled through services such as the monitoring of critical assets with a SIEM technology. Monitoring of critical assets is also a requirement as expressed by various international authoritative and normative documents – such as acts, standards and regulations. The requirement for the monitoring of critical assets are expressed in various authoritative and normative sources. Some examples of these authoritative and normative sources requirements may be found in:

- COBIT 4.1 - DS5.5 Security testing, surveillance and monitoring [134].
- IITIL v3 - SO 5.13 Information security management and service operation [135].
- ISO/IEC 27002:2005 - 10.10.2 Monitoring system use, 10.10.3 Protection of log information, 10.10.4 Administrator and operator logs, 15.3.1 Information systems audit controls [135].
- SANS Critical controls - Critical control 14: Maintenance, monitoring, and analysis of security audit logs [51].
- NIST SP 800-53 - 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) [136].

- Payment card industry- Data security standard (PCI-DSS) [177],
- ISO/IEC 27001:2005 [178],
- South African ECT Act [118],
- Sarbanes Oxley (SoX) [179] and others [180].

Kelley and Moritz [181] list the ability to monitor and respond to threats as the primary functions of SOCs. These functions are supported as primary functions in literature by Milne [182] Dempsey; Johnson; Scholl and Stine [183] and Rothke [170]. Paganini [161] describes a SOC as a structure that "continuously monitor and improve an organization's security posture while preventing, detecting, analysing, and responding to cyber security incidents with the aid of both technology and well-defined processes and procedures."

During the European Chief Information Security Officer (CISO) Information Security Workshop in 2013, it was concluded that a SOC's responsibility spans the daily operations of security events [184], while Zimmerman [185] defines a SOC as "a team primarily composed of security analysts organized to detect, analyse, respond to, report on, and prevent cybersecurity incidents." Kelley *et al.* [186] explains that one of its functions is to "…monitor(s) and manage(s) all aspects of enterprise security in real-time from a single, centralized location."

Zimmerman [185] defines a SOC as "a team primarily composed of security analysts organized to detect, analyse, respond to, report on, and prevent cybersecurity incidents." while Kelley and Moritz [181] describe the purpose of a SOC as being that of an entity 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."

McAfee describes an SOC as an entity that is [187]

> ":…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."

In turn, Anderson describes a SOC as something dedicated to investigate, detect and respond to log events. These events could be triggered by security related correlating logic, using people, processes and technology [188].

As secondary functions, SOCs should provide information on latest threats and vulnerabilities as well as information on security countermeasures [181] [183]. SOCs should further be able to provide reporting and visualisation, strategic advice and guidance and vulnerability management as functions, [19]. Most

organisational cybersecurity operations could be offered from mature SOCs, including security device management.

The SOC functions, as taken from Zimmerman [185] and IBM [189] are shown in Table 32. We have used our experience in the planning, building and running of SOCs to map the similar functions as expressed by Zimmerman and IBM, both of which are authoritative sources in their field [190]. Our experience further supports the list of primary functions as presented by Zimmerman [185] and IBM [189].

**Table 32: SOC Functions**

| Zimmerman | IBM |
|---|---|
| Real-time monitoring. | Security and threat monitoring. |
| | Personnel recruitment, retainment and management. |
| Sensor tuning and management and SOC infrastructure operations and maintenance (O&M), SOC tool engineering and deployment. | Process development and optimisation |
| Cyber intelligence collection and analysts. | Emerging threat strategy (threat intelligence). |
| Triage or incident analysis, coordination and response. | Security incident management. |

We will be using the mapped functions from these two authoritative sources as the SOC primary functions for consideration during the development of the E-CMIRC. This list must not be seen as a complete list of SOC functions. Jacobs (2015) [138] has identified a comprehensive list of SOC functions, but we keep our selection of primary functions minimal on purpose as our intention is only to illustrate the application of levels 3 to 6 of the NCMF to develop the E-CMIRC.



SOCs also offer secondary functions such as security awareness training, and business impact assessments [138]. Taking the fact into consideration that the functions are selected to illustrate the development of the E-CMIRC, the secondary functions will be ignored. We have used our experience to aggregate the function descriptions from Zimmerman and IBM. The SOC primary functions are displayed in Table 33:

**Table 33: SOC Primary Functions**

| SOC primary functions | Aggregated From Table 32 |
|---|---|
| **Monitoring and evaluation.** | Aggregated from security and threat monitoring and real-time monitoring. |
| **Security operations.** | Aggregated from process development and optimisation, and sensor tuning and management, SOC infrastructure operations and maintenance (O&M), SOC tool engineering and deployment. |
| **Threat and vulnerability management.** | Aggregated from security and threat monitoring, emerging threat strategy (threat intelligence) and cyber intelligence collection and analysts. |

| | |
|---|---|
| **Incident handling.** | Aggregated from security incident management, and triage or incident analysis, coordination and response. |

The SOC monitoring and evaluation service satisfies the similarly named general national *monitoring and evaluate* function, while the SOC's incident handling service corresponds to the primary function of a CSIRT (incident handling) as introduced in Section 4.6.7. It also satisfies the general national *incident handling* function. These functions are offered by both internal and organisational SOCs, and MSSPs. It is our experience that SOCs are internally focussed in terms of the incident handling service, in that it only considers organisational or government department specific incidents. This leads to our discussion on SOC service delivery models.

## B4 SOC Delivery model selected for E-CMIRC

As stated in Chapter 2, service delivery realises benefits, and deliver on functions, and one of the benefits of selecting the correct service delivery model is that it aligns technology and processes.Taking into consideration that the E-CMIRC will be a combination of SOC and CSIRT services and technologies, and that it is meant for implementation at national level in developing countries, the MSSP model is selected as the most appropriate cybersecurity service delivery model for the E-CMIRC.

Our motivation for selecting the MSSP service delivery model is that its processes and technologies caters for disparate organisations and their requirements – this model is flexible enough to operate at national level, and to cater for different, geographically dispersed state departments nationally, all of which could potentially use different technologies and diverse processes. The selection of the MSSP model is further motivated by the fact that it caters for different clients across different sectors and industries. This imposes a technical requirement on the SOC primary technology, the SIEM, in that it needs to cater for multi-tenancy, and be able to segregate sensitive information from different clients or constituents. The MSSP service delivery model demands logical segregation of events and information, ensuring that events or information from different clients (or state departments) is never contaminated with one another.

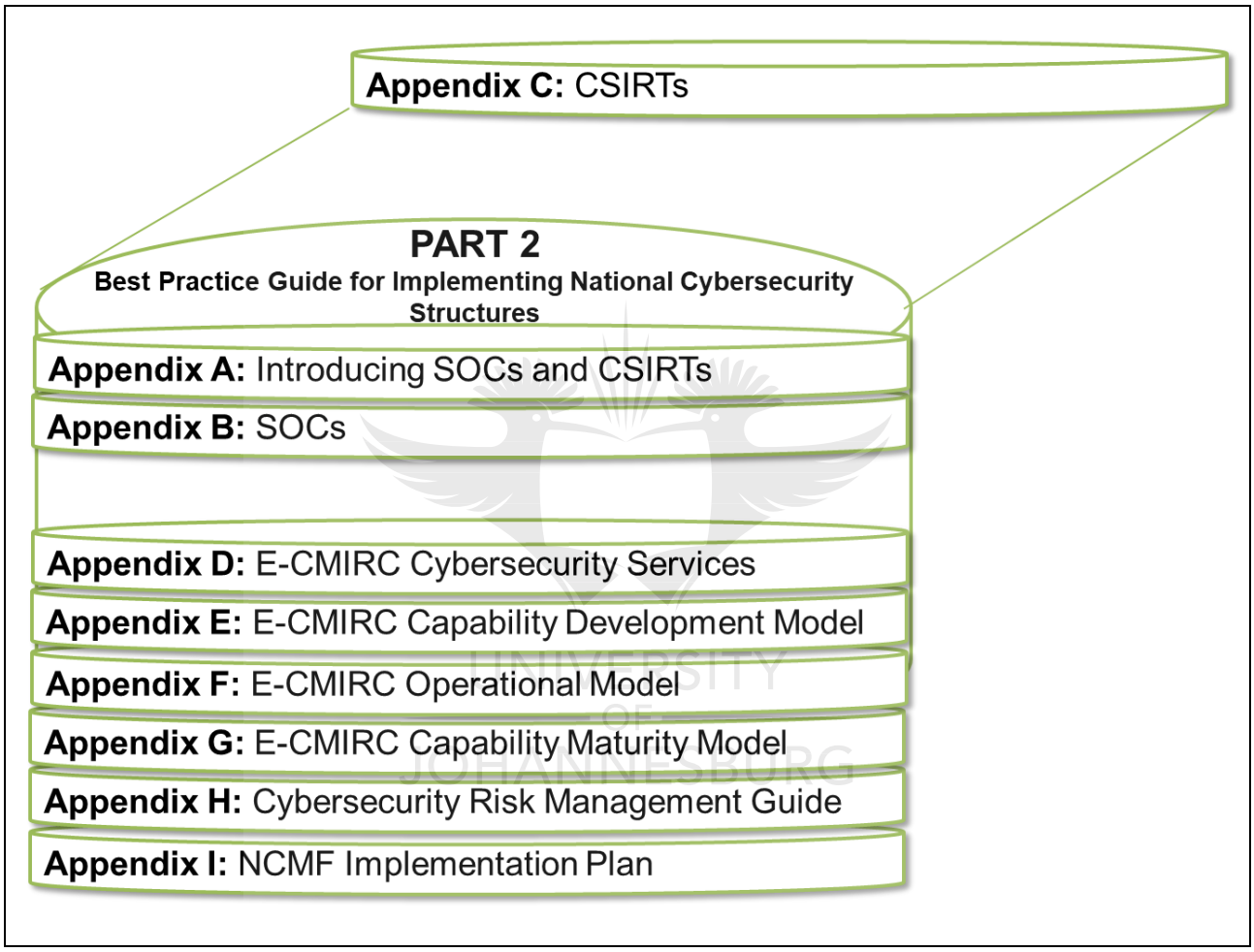
The E-CMIRC, serving at national level, and catering for different departments and constituents, will make use of this cybersecurity service delivery model to ensure that as many as possible national state departments and constituents are covered, taking into consideration requirements such as multi-tenancy and segregation. This is impossible to achieve with an organisational specific, internal SOC catering for, and focussing on only one client.

## B5 Conclusion

Appendix B considered the *monitoring and evaluation* function's structure, the SOC. SOC high-level functions were introduced and its primary functions are:

- Monitoring and evaluation.
- Security operations.
- Threat and vulnerability management.
- Incident management.

Available SOC service delivery models were introduced. The two models are internal or organisational SOCs, and MSSPs. The MSSP model was selected and motivated as appropriate for the E-CMIRC. In Appendix C, the *incident handling* function's structure, the CSIRT, is introduced.


Appendix C: CSIRTs
PART 2
Best Practice Guide for Implementing National Cybersecurity Structures
Appendix A: Introducing SOCs and CSIRTs
Appendix B: SOCs
Appendix D: E-CMIRC Cybersecurity Services
Appendix E: E-CMIRC Capability Development Model
Appendix F: E-CMIRC Operational Model
Appendix G: E-CMIRC Capability Maturity Model
Appendix H: Cybersecurity Risk Management Guide
Appendix I: NCMF Implementation Plan

# Appendix C: CSIRTs

## C1 Introduction

In Appendix B, we introduced the *monitoring and evaluation* function's structure, the SOC. In addition, the SOC primary functions and service delivery models were introduced. The SOC service delivery model most suited to the E-CMIRC was then identified and motivated as the MSSP model. Appendix C introduces the *incident handling* function's structure, the CSIRT. The purpose of this chapter is to identify the CSIRT functions, its service delivery models as well as its authority levels. The authority levels describe the type of powers a CSIRT can exert over its stakeholders, and authority levels will be applied to, and described in terms of the E-CMIRC. In this appendix, We will select and motivate a CSIRT structure, type and service delivery model that can be used for the E-CMIRC.

The *incident handling* function and its structure, the CSIRT, is discussed in more detail than the *monitor and evaluate* function's structure, the SOC. Our motivation for spending more time on the CSIRT structure is as follows:

- There are more reference implementations and literature available for CSIRTs at national level. This is important, and we will use this knowledge since the E-CMIRC is envisioned as a national structure.
- Our research showed that it is not common for SOCs to be deployed at national level. CSIRTs are more often deployed at national level, and we will make use of their national deployment models to apply to our E-CMIRC.
- The CSIRT national and government implementation structures and types will be used as a foundation during the development of the E-CMIRC structure
- The focus of national and government CSIRTs are on improving the national security posture, while the focus of SOCs is more commonly on improving organisational security posture.

The rest of the chapter is broken up as follows:

**Section C2** introduces the CSIRT structure and functions. The CSIRT structure and type influences the functions offered by the CSIRT.

**Section C3** introduces and motivates the CSIRT delivery model, and a selection is made for the E-CMIRC. This further influences the selection of functions and services for the E-CMIRC.

**Section C4** introduces and he CSIRT types, and a selection is made for the E-CMIRC. The CSIRT types further influences the selection of functions and services for the E-CMIRC.

**Section C5** selects and motivates the CSIRT Service Delivery Model Selected for our E-CMIRC

**Section C6** introduces the authority levels that can be exerted by CSIRTs, and these will be made applicable to the E-CMIRC. This determines the level of authority the E-CMIRC will be able to exert over its constituents.

**Section C7** introduces the E-CMIRC functions.

**Section C8** concludes this chapter.

## C2 Introducing CSIRT Structures and Functions

The CSIRT structure and type influences its functions, which, in turn influences its services. The service delivery model of the CSIRT further determines its place within an organisation or nation state, and could also influence its placement in terms of the geographical or physical location. CSIRTs functions are typically offered from a single local structure, or a distributed structure across an organisation or nation [145]. It is our experience that the CSIRT structure's location (local, distributed, national, and organisational) influences the type of services it offers.

For example, it is our experience that the services offered by a national, distributed CSIRT structure with a presence in rural areas, will offer different services to those than its parent CSIRT in a town or city. In rural areas, aspects like access to technology, and access to the internet could be a challenge, thus, a rural CSIRT structure would potentially only offer services and capabilities such as awareness campaigns, as opposed to multiple services offered by its parent CSIRT.



Another example is that a CSIRT located within an urban area, with access to skilled resources and communication channels, will offer its services differently to a CSIRT in a rural area with little or no access to skilled resources. A CSIRT with skilled resources may also offer services that may not even be considered by a lesser skilled CSIRT. The structure and type eventually influence the selection of services to be offered from a CSIRT, and this is important for us as the identification of a CSIRT structure and type will assist us with the identification of services for our E-CMIRC.

ENISA typifies CSIRT structures by the services they provide [191], or by the sectors they serve [192]. We will use the CSIRT type and sector to guide us during the identification of CSIRT structures. CSIRTs' services may be offered from national or organisational structures. ENISA mentions four different ways a CSIRT may be structured [193]. These are all organisational models, and do not reflect a national capability. The four different ways of structuring a CSIRT according to ENISA are [193]:

- The CSIRT structure as an independent organisation with its own staff.

- The CSIRT structure as part of an existing organisation.
- Campus, or distributed model.
- Voluntary model where people or groups with a shared interest get together and provide advice and support to each other.

The common aspect here is that all these structures offer the *incident handling* function. The General Secretariat of the Organisation of American States (OAS) [126] recommends that CSIRTs be structured or classified according to the sector, or community in which they are active [126]. Some examples are academic CSIRTs, commercial CSIRTs, critical infrastructure CSIRTs, government CSIRTs, national CSIRTs and military CSIRTs to name a few. These structures are also supported by Killcrece; Kossakowski; Ruefle and Zajicek [145]. The Software Engineering Institute at the Carnegie Mellon University has categorised CSIRTs into six different structures These are [194]:

- Internal CSIRTs.
- National CSIRTs.
- Coordination centres.
- Analysis centres.
- Vendor teams.
- Incident response providers.

Skierka; Morgus; Hohmann and Maurer (2015) [195] developed a CSIRT classification typology focusing on the community and organisational model of the CSIRT. This was done as part of a joint project between New America and the Global Public Policy Institute (GPPi). ENISA developed two typologies - and their focus is on the environment in which the CSIRT operate. The differences and similarities are shown in Table 34 as taken verbatim from [195] in order not to change the intent and meaning.

**Table 34: CSIRT Classification Typologies [140]**

| GPPI / New America (2015) | ENISA (2013) | ENISA (2006) |
|---|---|---|
| **Regional** | Not applicable | Not Applicable |
| **National** | National/governmental<br>National<br>De facto national | National CSIRT |
| **Sectoral** | Research and education<br>Financial sector<br>Energy sector<br>Industrial sector | CIP/CIIP sector-CSIRT<br>Governmental sector-CSIRT<br>Military sector-CSIRT |
| **Organisational** | Governmental | Academic sector-CSIRT |

| | | |
|---|---|---|
| | Governmental/military<br>Non-commercial organisation<br>Commercial organisation | Internal CSIRT<br>SME CSIRT |
| **Vendor** | ICT vendor customer base<br>Service provider/ISP customer base | Vendor CSIRT |
| **Commercial** | Not applicable | Commercial CSIRT |

Since the intention is for the E-CMIRC to offer the *monitoring and evaluate* and *incident handling* functions at national level, we will exclude organisational and campus CSIRTs, and only consider the national and government CSIRTs. We have further stated that our intention is for the E-CMIRC to serve as a national structure, improving the national cybersecurity posture. This means that the E-CMIRC will provide a national *incident handling* function to the nation, inclusive of government. We have also determined that most authoritative literature[8] makes reference to government and national CSIRTs, and this means that we will have enough reference implementations and sources to consult. We thus select the national CSIRT and the government CSIRT as reference structures for the E-CMIRC.

National CSIRT performs incident handling and coordination at national level. It is the top-level structure, and all other sector-CSIRTs report to the national CSIRT. The government CSIRT serves the government and its organs. There exists a reciprocal relationship between the national and government CSIRTs in that they collaborate and share information. We will now introduce the CSIRT structures as defined by the OAS.

**National CSIRT:** In addition to serving a defined community, a country's National CSIRT usually takes on the role of national coordinator for incident response, and is the contact point for national and international incidents. The role and target community of a national CSIRT varies depending on its roles and the existence of other response centers. For example, if there is no CSIRT designated for critical infrastructure, the national CSIRT could assume responsibilities normally assigned to a critical infrastructure response team. It can be considered as a "last resort CSIRT," or one which takes charge of incident response matters that are not under the purview of another body. It is very common for various CSIRTs to be part of the community the National CSIRT serves.

**Government CSIRT:** Government CSIRTs serve state institutions in order to ensure that government IT infrastructure and the services it facilitates to citizens have an adequate level of security. Government CSIRTs adapt their structures to the Government. They can meet local, regional or sector-specific government communities. Government CSIRTs can operate independently or interact to combine strategies and efforts and share resources and knowledge. Within a country, for example, the Ministry of Education and the Ministry of Tourism might operate independent CSIRTs, but collaborate and share information regularly.

[8] In this context, the authoritative literature refers to peer reviewed literature, or publications by people or entities that are seen as authoritative and experts in their field. It should not be confused with authoritative sources.

## C3 CSIRT types

Now that we have introduced the CSIRT structures, we also need to introduce the CSIRT types. The CSIRT types are different from the CSIRT structures in that the types define the characteristics of the CSIRT, while the structure describes how the CSIRT is organised. Both the CSIRT types and structures influences the CSIRT services. The OAS defines four different CSIRT types. The types are:

- Localised security team.
- Distributed incident response teams.
- Coordinating team.
- Centralised incident response team.

West-Brown, Stikvoort; Kossakowski; Killcrece; Ruefle and Zajicek [191] identify three different types of CSIRTs, which can be structured according to any of the models described by ENISA [193]. The types of CSIRTs described by Stikvoort *et al* [191] are:

- International coordination centre.
- Corporation.
- Technical.

In keeping with the intention of the E-CMIRC to provide services at a national level, the centralszed incident response team type is selected as most appropriate for the intended use of the E-CMIRC, based on its characteristics. The centralised incident response team is a single team responsible for the management and response of security incidents across a number of locations that belong to one larger organisation. This model would be appropriate, for example, in an enterprise. In these structures, there is a defined response team and dedicated staff trained in managing information security and responding to security incidents.

The centralised incident response team type is scalable, and its characteristic is to provide a geographically dispersed *incident handling* function. Considering the South African context, and as stipulated in the NCPF [33] and Cybercrimes and Cybersecurity Bill [34], the Cybersecurity Hub serves as the national CSIRT, and the SSA's ECS-CSIRT serves as the government CSIRT [83]. Section C5 explores the high-level functions of national and government CSIRTs.

## C4 CSIRT functions

A national CSIRT could serve as a government CSIRT [195]. This means that an overlap may be found between the services offered by national and government CSIRTs. Nation states however often detach government CSIRTs and national CSIRTs. This also the case in South Africa where the national CSIRT

(Cybersecurity Hub) is not under the explicit control of the government, and its function is largely coordinating and advisory [33].

It is our experience that the government CSIRT (ECS-CSIRT) has control to some degree over the networks and its connections within its constituency. The use of a government CSIRT often matures into a tactical cyber crisis management service [1]. In terms of the South African context, the Cybersecurity Hub was established by the DTPS. The functions of the Cybersecurity Hub according to the NCPF are listed verbatim, as taken from [33]:

- Coordinate general cybersecurity activities.
- Disseminate relevant information to other sector-CSIRTs, vendors, and technology experts on cybersecurity developments.
- Provide best practice guidance on ICT security for the government, business and civil society.
- Initiate cybersecurity awareness campaigns.
- Promote compliance with standards, procedures and policy.
- Encourage and facilitate the development of appropriate additional sector-CSIRTs.

The establishment of sector-CSIRTs is also a key function of the Cybersecurity Hub. Another function of the Cybersecurity Hub is to serve as a coordinating centre between national structures, sector-CSIRTs, and the public. At the time of writing, South Africa had only one established sector-CSIRT for the banking sector.

This banking sector-CSIRT was established, and operated by the South African Banking Risk Centre (SABRIC), that currently has 19 member-banks. SABRIC is a non-profit organisation and their aim is to assist banking and cash- intransit companies in the fight against organised bank related crimes, and this includes organised crime in the cyber domain [196].

This model of operation is displayed in Figure 35, showing that there is a reciprocal information sharing relationship between the Cybersecurity Hub, the ECS-CSIRT, Cyber Command and Cybercrime Centre. It further shows that organisational CSIRs report to sector-CSIRTS, that, in turn report to the Cybersecurity Hub.

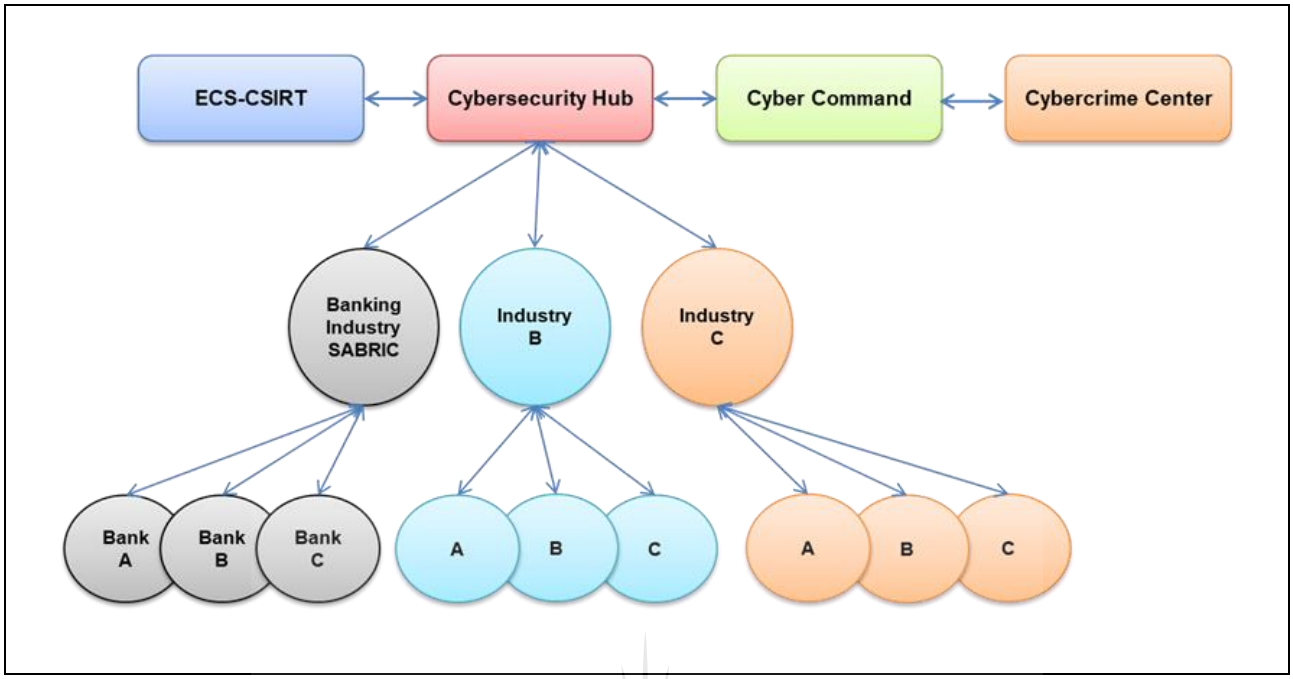



**Figure 35: Relationship between the Cybersecurity Hub, national structures and sector CSIRTs**

CSIRT functions as expressed by the Internet Engineering Task Force (IETF) in request for comment (RFC) 2350 [197] and the SANS Institute [198] are listed verbatim in Table 35. The IETF and SANS functions were selected as they are representative of all the CSIRT functions as mentioned in their definitions in the preceding literature. Some of these functions are also described as functions for the Cybersecurity Hub. We have grouped the CSIRT functions based on their relevance to each other, and based on our experience. This is done to determine the CSIRT functions, as well as illustrate differences and similarities between the IETF and SANS description of CSIRT functions.

**Table 35: CSIRT Functions**

| **IETF** [197] | **SANS** [198] |
|---|---|
| Remediate security activity in their constituency | Real-time incident response activities and non-real-time incident response activities |
| Manages the entire incident life-cycle<br>Play a coordination role to resolve incidents | Provide incident handling capabilities within an organisation |
| Analysis of incidents and vulnerabilities | Analysis of incidents and vulnerabilities |
| The CSIRT will otherwise share information freely when this will assist others in resolving or preventing security incidents | For any CSIRT to be effective, it needs information and strong, positive communications with its constituency |

A national CSIRT's main role is to coordinate interaction between government and actors, and to promote incident handling effectiveness. This is achieved through coordinating incident handling efforts, and by promoting collaboration between government and actors. The national CSIRT structure further provides services such as the analysis of incidents and vulnerabilities, and disseminates and share information. It also develops best practices and supports government in the development of national best practices.

We can thus conclude that the primary functions of a national CSIRT are to offer an *incident handling* function (national or organisational) by means of promoting and enabling cooperation and coordination between stakeholders, provide guidance in terms of cybersecurity issues and influence national policy, as well as the dissemination and sharing of cybersecurity information at national level. It may also assist in establishing awareness programmes at national level. The primary CSIRT functions aggregated from the IETF and SANS are thus:

**Table 36: CSIRT primary functions**

| CSIRT Primary Functions | Aggregated from Table 35 |
|---|---|
| **Incident handling function.** | • Remediate security activity in their constituency<br>• Real-time incident response activities and non-real-time incident response activities<br>• Manages the entire incident life-cycle<br>• Play a coordination role to resolve incidents<br>• Provide *incident handling* capabilities within an organisation |
| **Analysis of *incidents and vulnerabilities* function** | • Analysis of *incidents and vulnerabilities* |
| **Disseminate and *share information* function** | • The CSIRT will otherwise share information freely when this will assist others in resolving or preventing security incidents<br>• For any CSIRT to be effective, it needs information and strong, positive communications with its constituency |

## C5 CSIRT service delivery model selected for E-CMIRC

As stated in Appendix A, the *incident handling* function may be seen as a highly specialised, highly mature, sub-function of the SOC's (which offers the *monitoring and evaluation* function), or the *monitoring and evaluation* function may be viewed to serves as input, and feeding into the *incident handling* function. We have made a conscious decision to view the *monitoring and evaluation* function as the primary function of our E-CMIRC since our intention is to protect a nation's cyberspace through monitoring for cyber-attacks and threats, by first detecting them (events), and then responding once the events are classified as incidents.

The *monitoring and evaluation* function will thus be used to detect attacks and threats, and the *incident handling* function will be used to respond to incidents resulting from those attacks and threats. The *monitoring and evaluation* function happens first (detection), and its results are then passed to the *incident handling* function for response and resolution. Taking the above statement in consideration, the *incident handling* function will serve as a highly specialised, highly mature, sub-function of the *monitoring and evaluation* function, to be offered from the E-CMIRC.

In Appendix B and Appendix C stated that the SOC and CSIRT service delivery models will have an influence on the services they offer, and, ultimately, the technologies and processes needed to support those services. The CSIRT service delivery model that we have identified as most suitable and complementary for the E-CMIRC, is that of a National and Government CSIRT [194], with the centralised incident response team as type, and *incident handling, analysis of incidents and vulnerabilities and disseminate and share information* functions [126]. This is shown in Table 37:

**Table 37: CSIRT structure, type and function for E-CMIRC**

| | |
|---|---|
| **CSIRT Service Delivery Model** | National and government |
| **CSIRT Type** | Centralised incident response team |
| **CSIRT Function** | Incident handling<br>Analysis of incidents and vulnerabilities function<br>Disseminate and share information function |

We have motivated the selection of the national and government CSIRT structures and centralised incident response team type as relevant for the E-CMIRC, keeping in consideration that we are developing it to provide a national cybersecurity function, and also because there is a wealth of reference implementations available. The reference implementations have been proven as successful in improving the cybersecurity posture of nation states [2] [199] [200].

Section C6 presents the CSIRT authority levels. The CSIRT authority levels describe the possible powers the CSIRT may exert over its constituents, and this authority is an important consideration for the E-CMIRC, and assists with clarifying its authority level at national level.

## C6 CSIRT authority levels

The CSIRT authority level describes the type of powers a CSIRT can exert over its constituents. This also determines the CSIRT's obligations in terms of the *incident handling* function [126]. These authority levels are important, since they will serve as guidance when nations need to determine the level of authority the E-CMIRC can exert over its constituents. The levels of authority, which can be exerted by CSIRTs, with our recommendations, are, as taken from [126]:

- **Full authority** – The CSIRT has authority to execute all steps and actions during the resolution of an incident. Actors and constituents are required to implement the measures as stipulated by the CSIRT. The CSIRT further has full control over any internal cybersecurity related incidents. We recommend that the E-CMIRC exert full authority where it concerns cybersecurity incidents at international and national level.

- **Shared authority** – decisions regarding incidents are made jointly between the CSIRT and its affected actors and constituents. The CSIRT supports actors and constituents with equipment and expertise. It is recommended that the E-CMIRC exert shared authority where it concerns commercial actors and constituents, such as the banking and financial sector.

  The E-CMIRC will provide expertise and advice where it concerns cybersecurity related incidents. The E-CMIRC also offers shared authority where it concerns other government entities. From a South African context, this means members of the Justice, Crime Prevention and Security (JCPS) cluster, such as the Department of Defence (DOD) and Department of Justice (DOJ).

- **Null authority** – the CSIRT has no jurisdiction over decisions where it concerns incidents. Advice, guidance and expertise are provided, but those affected take the decisions. We recommend that the E-CMIRC exert no authority where it concerns the resolution of public cybersecurity related incidents. Public cybersecurity related actors and constituents, such as managed security service providers, (MSSPs), and vendors such as Microsoft and other cybersecurity service providers, could potentially resolve incidents. Depending on the maturity level of the E-CMIRC (the E-CMIRC capability maturity model is developed in Appendix G), the E-CMIRC can do a satisfaction survey, and, also perform quality checks.



- **Indirect authority** – The CSIRT has no authority over actors and constituents, but can influence them through regulatory bodies with which the CSIRT has an established trust relationship. We recommended that the E-CMIRC exert indirect authority over sectors and industries through regulatory bodies where it concerns the establishment of sector-CSIRTs. At this level, incidents are viewed as operational issues that must be resolved internally, but the E-CMIRC may influence behaviour through regulatory bodies.

  The E-CMIRC has no authority where it concerns the handling and resolution of public incidents. The E-CMIRC thus primarily serve as a government CSIRT, offering some of the services and functionality of a national CSIRT, but to the exclusion of the resolution of publicly reported incidents. From a South African context, a good example is using the Independent Communications Authority of South Africa (ICASA) to drive the establishment of a telecommunications sector-CSIRT.

The chosen levels of authority and their applicability to the E-CMIRC is shown in Figure 36. Figure 36 shows that the full authority for the E-CMIRC means that it would be responsible for all national (inclusive of government) and international incidents across the incident management lifecycle. The E-CMIRC shares authority where it concerns incidents at the JCPS cluster, constituents and sector-CSIRTs. The E-CMIRC has indirect authority where it concerns incidents at government and sector-CSIRT level.

Figure 36 shows that the full authority for the E-CMIRC means that it would be responsible for all national (inclusive of government) and international incidents across the incident management lifecycle. The E-CMIRC shares authority where it concerns incidents at the JCPS cluster, constituents and sector-CSIRTs. The E-CMIRC has indirect authority where it concerns incidents at government and sector-CSIRT level.

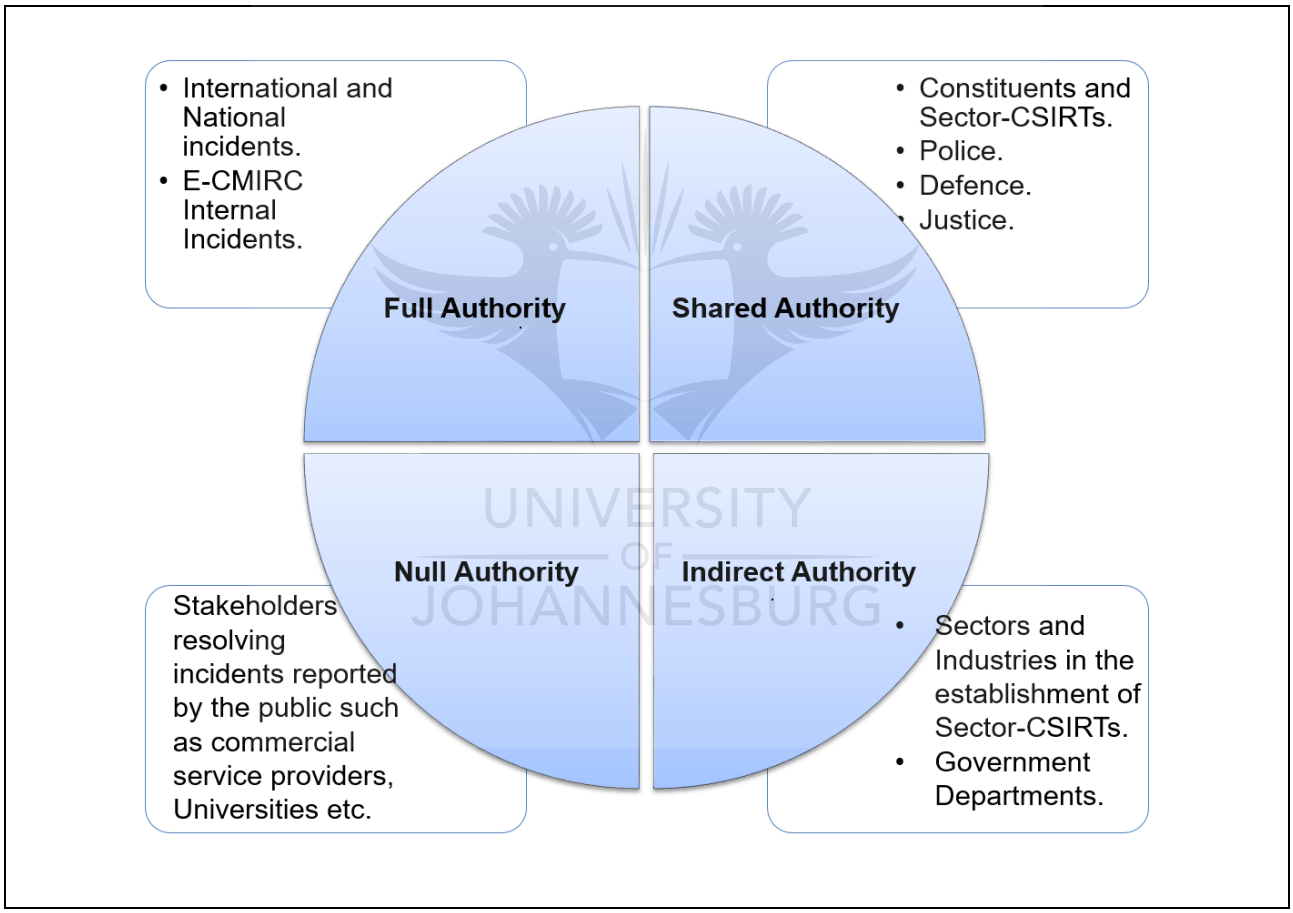



**Figure 36: E-CMIRC levels of authority**

We will now consider the SOC and CSIRT functions, and identify overlaps and similarities between them. Our motivation for doing so is that it will allow us to determine if there are overlaps in services, and their processes and technologies. Our intention is then to combine these services and technologies, and offer them from the E-CMIRC to realise a cost and skills saving.

## C7 E-CMIRC functions

We identified thirteen of the most general cybersecurity functions in Chapter 4, and selected the *monitoring and evaluation* and *incident handling* functions, to illustrate the implementation part of the NCMF by developing our E-CMIRC. The selection of the *monitoring and evaluation* and *incident handling* functions allowed us to identify its structures, the SOC that is used for the *monitoring and evaluation* function, and the CSIRT that is used for the *incident handling* function. These two structures have their own functions, and we identified those in Appendix B and Appendix C. We again stress the fact that there are two types of functions to consider – the national cybersecurity functions and then the structure specific functions. We now need to aggregate, and select the cybersecurity functions for our E-CMIRC from the SOC and CSIRT functions. Our journey up to the identification of SOC and CSIRT functions is shown in Figure 37.

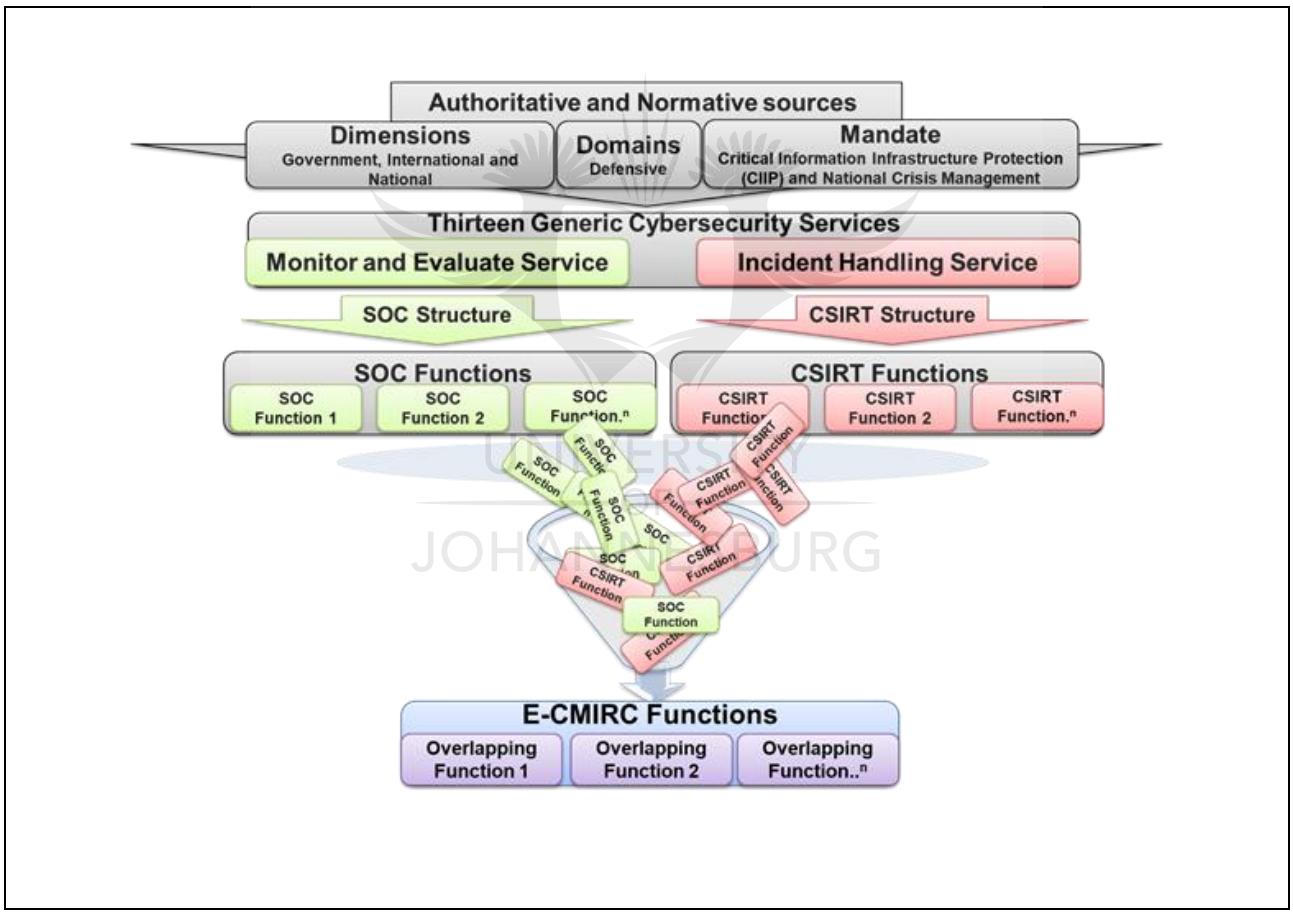



**Figure 37: SOC, CSIRT and E-CMIRC function selection**

Figure 37 shows that we have introduced and identified the authoritative and normative sources, as well as elements influencing the identification, selection and prioritisation of cybersecurity functions. This was done in Chapter 3. Authoritative and normative sources were identified, and the government, national and international Dimensions were used to identify actors.

We have selected and motivated for the defensive domain, the critical information infrastructure protection (CIIP), and the national crisis management mandate to be used for our E-CMIRC. All these elements helped us to identify SOC s and CSIRTs as the structures offering these functions. The overlapping and similar SOC and CSIRT functions will then be identified and offered from the E-CMIRC.

We also identified the SOC primary functions in Appendix B. To recapitulate, the identified SOC primary functions, as supported by Kelley *et al* (2006) [181]; Milne (2005) [182]; Dempsey *et al* (2011) [183]; Rothke (2009) [170]. Paganini (2016) [161]; Zimmermann (2014) [185] and IBM (2016) [189] are:

- Monitoring and evaluation.
- Security operations.
- Threat and vulnerability management.
- Incident handling.

The CSIRT cybersecurity primary functions were identified in Appendix C. The CSIRT cybersecurity primary functions as expressed by the SEI at CMU [150]; ENISA [148]; Morgus *et al*. (2015) [149]; ENISA [193]; Brownlee [197]; SANS) Institute [198]; and IETF in RFC 2350 [197] is:

- Incident handling.
- Analysis of incidents and vulnerabilities function.
- Disseminate and share information function.



The SOC and CSIRT functions are shown in Table 38. We have done a mapping of the SOC and CSIRT functions based on our experience.

**Table 38: E-CMIRC functions**

| SOC Functions | CSIRT Functions |
|---|---|
| Monitoring and evaluation function | |
| Security operations function | |
| Threat and vulnerability management function | Analysis of incidents and vulnerabilities function<br>Disseminate and share information function |
| Incident handling function | Incident handling function |

This functional overlap is shown in Table 38. It illustrates that there is an overlap between SOC and CSIRT primary functions. The unique function are the SOCs *monitoring and evaluation function*, and *security operations* function. There exists an overlap between the rest of the SOC and CSIRT functions. The primary difference in the delivery of functions, and their services when comparing the SOC MSSP service delivery model,

with the CSIRT national and government service delivery model, is that the SOC functions' services are internally focussed whereas the CSIRT functions' services are externally focused. For example, a SOC will provide its services to one customer at a time, with no information and organisational specific threat intelligence sharing between customers. A CSIRT, on the other hand, will foster information sharing between constituents and industries. Internationally recognised standards and frameworks such as ITIL, COBIT and ISO/IEC 27001:2013 [135] also support the overlaps and similarities between these functions. We will use a combination of SOC and CSIRT functions to be offered from the E-CMIRC. The functions we have selected for the E-CMIRC are:

- Monitoring and evaluation function
- Security operations function.
- Threat and vulnerability management function.
- Incident handling function.

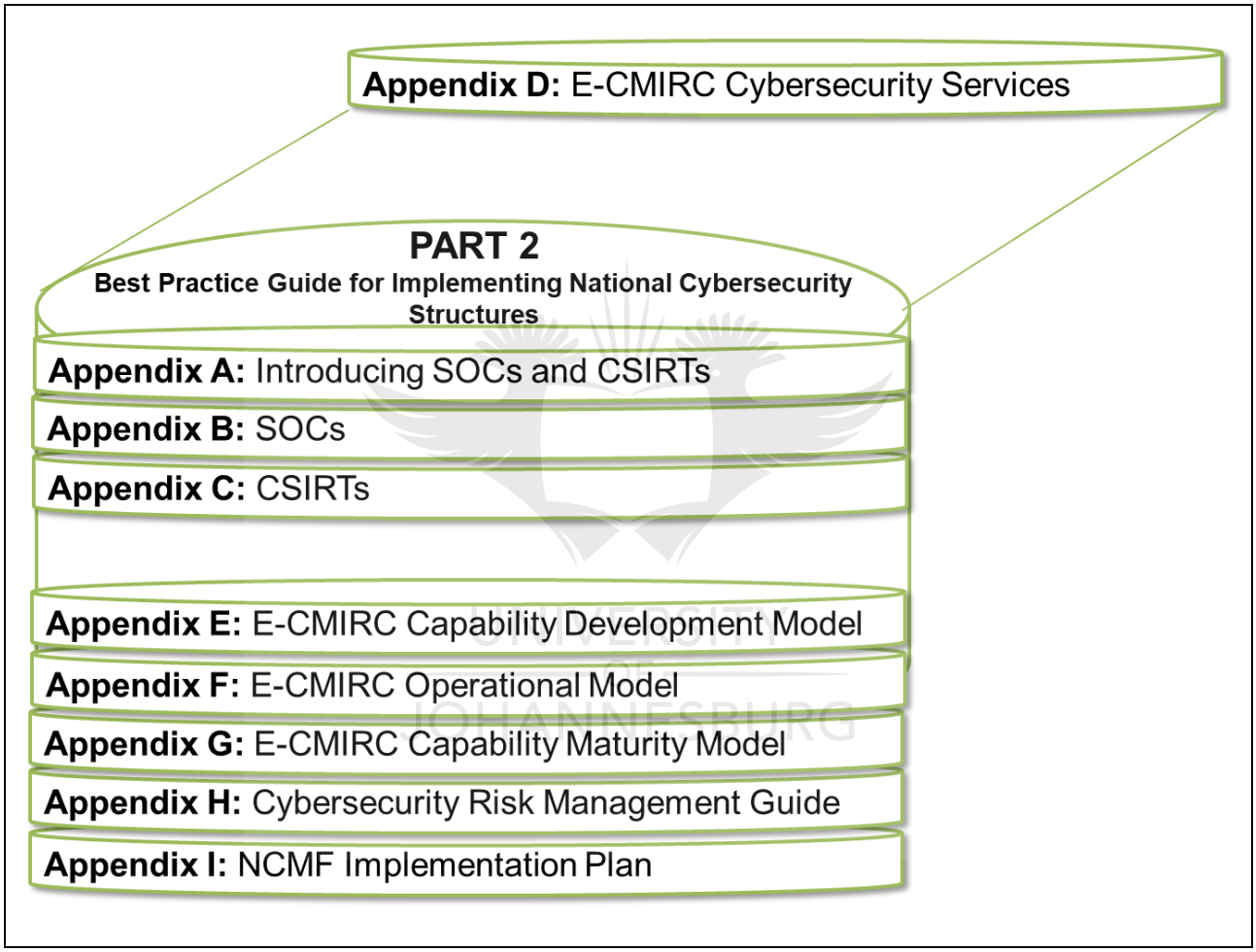
Our motivation for selecting these functions is that they deliver on the two selected general cybersecurity functions of *monitoring and evaluation*, and *incident handling*. In Appendix D, we will identify the services.of the SOC and CSIRT functions. These services are then analysed, and similar, or overlapping services are mapped back to the E-CMIRC functions. We have now selected and motivated the E-CMIRC cybersecurity functions, and can now progress to the identification of its services in Appendix D.

## C8 Conclusion

The CSIRT structures were described in this appendix in which we introduced two CSIRT structures as described in various literature sources as national, and government CSIRTs. The national and government CSIRT structures were then selected and motivated as most relevant for our E-CMIRC taking in consideration its intended application. The intention is for the E-CMIRC to primarily serve as a government type CSIRT, but with some of the functionalities and services of a national CSIRT, and a SOC.

We also introduced the CSIRT types, and selected the centralised incident response team type's characteristics as most relevant for our E-CMIRC. The CSIRT types were discussed in Section C4. We then considered some of the definitions for national and government CSIRTs, and found confirmation in authoritative literature sources that the *incident handling* function is one of the primary functions of a CSIRT. We then presented the service delivery model selected for the E-CMIRC in Table 37. The different CSIRT authority levels were introduced, and recommendations made for the E-CMIRC in Section C7. We have correlated SOC and CSIRT functions for the E-CMIRC in Section C8, and presented and motivated functions for the E-CMIRC.

Our rationale for identifying the CSIRT service delivery model, structure and types is that they offer different functions. We have selected a CSIRT service delivery model, structure and type for the E-CMIRC, and from there identified its relevant functions. In turn, the identification of the functions allows us to identify the services of the functions. In Appendix D, we will identify the SOC and CSIRT services, and map them back to the selected E-CMIRC functions. From there, we will identify similar services, and services sharing the same processes and technologies.


Appendix D: E-CMIRC Cybersecurity Services
PART 2
Best Practice Guide for Implementing National Cybersecurity Structures
Appendix A: Introducing SOCs and CSIRTs
Appendix B: SOCs
Appendix C: CSIRTs
Appendix E: E-CMIRC Capability Development Model
Appendix F: E-CMIRC Operational Model
Appendix G: E-CMIRC Capability Maturity Model
Appendix H: Cybersecurity Risk Management Guide
Appendix I: NCMF Implementation Plan

# Appendix D: E-CMIRC cybersecurity services

## D1 Introduction

Appendix D is dedicated to the identification of SOC and CSIRT services to deliver its functions. Accoirdingly, we will consult the available literature sources to identify the SOC and CSIRT services. Once we have identified the SOC and CSIRT services, we will map the services back to the E-CMIRC functions identified in Appendix C. We stated in Appendix C that the SOC and CSIRT service delivery model type and functions all have an effect on the services. The service delivery model, type and functions we have selected for the E-CMIRC is shown in Table 39.

**Table 39: SOC and CSIRT Service Delivery Models, Types and E-CMIRC functions**

| | SOC | CSIRT |
|---|---|---|
| **Service Delivery Model** | MSSP | National and government |
| **Type** | Multi-tenancy | Centralised incident response team |
| **E-CMIRC Functions** | Monitoring and evaluation function<br>Security operations function.<br>Threat and vulnerability management function.<br>Incident handling function. | |

The process we will follow to identify the SOC and CSIRT services is as follows:

- Identify SOC services in the authoritative literature.
- Identify CSIRT services in the authoritative literature.
- Map the SOC and CSIRT services to the E-CMIRC functions identified in Section D4.
- Identify common and unique SOC and CSIRT services.

The identified services will then be mapped to the E-CMIRC functions we identified in Appendix C We are doing this to ensure that our E-CMIRC functions map to services from existing and proven structures. This will provide us with a list of services that are needed to realise the E-CMIRC functions. The services are then compared, and common or similar services will be identified to be offered from the E-CMIRC. Our approach is displayed in Figure 38.

Figure 38 includes Figure 37 at the top, and it shows the process we have followed to identify the SOC, CSIRT and E-CMIRC functions. We have identified the SOC and CSIRT functions, and from these, selected and motivated functions for the E-CMIRC. These functions are realised by services, and we will identify SOC and

CSIRT services, and map those back to the E-CMIRC functions (which is a selection from SOC and CSIRT functions).

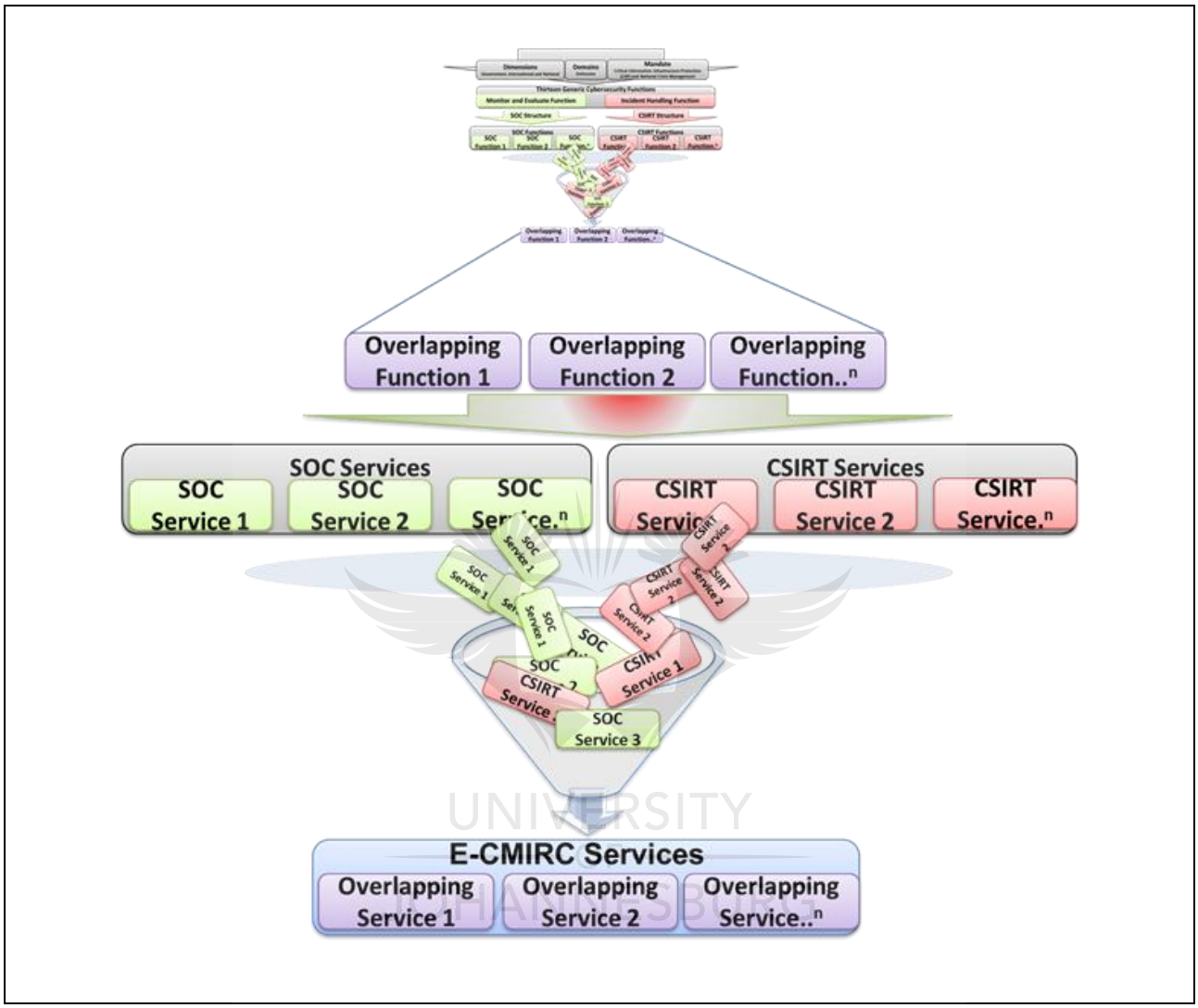



**Figure 38: SOC, CSIRT and E-CMIRC Service Selection**

We will now build on the E-CMIRC functions we selected in Appendix C, and in this appendix we will continue with the identification of SOC and CSIRT services. We will then map these services to the E-CMIRC functions and identify overlaps and similarities. This provides us with a list of services delivering the E-CMIRC functions. From this list, we will select and motivate services for the E-CMIRC to realise its functions. At the end of this appendix, we will have a list of E-CMIRC services delivering the E-CMIRC functions. The rest of the appendix is structured as follows:

**Section D1** introduces the SOC services as identified in authoritative sources.

**Section D2** introduces the CSIRT services identified using authoritative sources.

**Section D3** maps the SOC and CSIRT services to the E-CMIRC functions.

**Section D4** maps the SOC and CSIRT services to identify SOC and CSIRT common and unique services.

**Section D5** introduces the approach we will follow to select services for our E-CMIRC.

**Section D6** maps the E-CMIRC functions and defensive domain lifecycle phases to the list of SOC and CSIRT common and unique services. This provides us with a list of services for the E-CMIRC.

**Section D7** makes a proposition on how to monitor national security technical controls.

**Section D8** concludes this chapter.

## D2 SOC cybersecurity services

Although SOCs provide a cybersecurity operational function, an overlap of services does exist when compared with CSIRTs [201]. In order to identify and select services for the E-CMIRC, the cybersecurity services offered by SOCs and CSIRTs have to be identified first. Services common and unique to SOCs and CSIRTs are then determined. Jacobs *et al* [190] has identified SOC services, and these are supported by SOC service providers [202]; [203]; [204]; [205]; [206]; [207]; [208]; [209]; [210]; [211]. The SOC services are shown in Table 40.



**Table 40: SOC cybersecurity services**

| SOC Service | Description |
|---|---|
| **Counter intelligence** | Cyber counter intelligence is where a nation state uses cyber intelligence as a mechanism to identify, penetrate and neutralise foreign or hostile nation states. It also focusses on collecting foreign intelligence using traditional means as well as cyber means [212] |
| **Surveillance** | Cyber surveillance is the surveillance of people, objects or processes, using data networks. Nation states will practice surveillance to gather and analyse information, with the purpose of preventing cyber risks and attacks, to determine human behaviour, and to locate offensive nation states cyber warriors [213]. |
| **Providing strategic advice and guidance and integrated threat intelligence** | Threat intelligence considers emerging cyber threats to national assets. It provides evidence-based knowledge, and actionable advice to inform a nation states decision and response to national cyber threats. It contextualises, at a national level, threats, threat indicators, mechanisms and implications [214]. Integrated threat intelligence means that the threat intelligence tools and |

| SOC Service | Description |
|---|---|
| | technologies integrates with other tools such as SIEMs and helpdesk software. It includes aspects such as security knowledge management and security pre-warning. |
| **Incident response, incident management** | Cybersecurity incidents are unplanned events that threaten the confidentiality, availability and integrity of national or organisational cyber assets and infrastructure. It has a negative impact or consequence at organisational level, and is operational in nature [72], [215], [216], [217] |
| **Asset management and criticality rating** | ITIL v 3 defines asset management as "...the Process responsible for tracking and reporting the value and ownership of financial Assets throughout their Lifecycle. Asset Management is part of an overall Service Asset and Configuration Management Process." [218]. IT Asset management is made up of business practices covering all aspects of corporate or national assets, such as inventory, risk management and contractual responsibilities that makes up the lifecycle of national assets. It also includes aspects such as tactical and strategic decision making [219]. From a cybersecurity perspective, criticality ratings are assigned to organisational assets. It is our experience that following an asset management strategy, allows organisations and nations to know what assets they have, where it is, and how important it is. This, in turns, helps with strategic and operational decisions, as well as how much to spend on securing critical assets. |
| **Aggregation and analysis of intelligence data** | Analysing events is to systematically examine and evaluate events and its information to discover its causes and effects. Analysis assist with decision making in terms of the classification of events as incidents, and the handling of incidents [220]. A SIEM tool may facilitate the analysis of cybersecurity events. Aggregation in context of the *Monitoring and Evaluate* function means that all units are taken as a whole [221]. As an example, all similar events from the same IP address are aggregated, and presented as one event. This may save time and storage space, but care should be taken when deciding on the aggregation of events since aggregation may negatively affect forensics. |
| **Correlation of content intelligence data** | Correlation takes place where two or more variables fluctuate together. It implies that there is a relationship between two or more events [222]. An example is where a source IP address generate an event occurs on a firewall, and the same source IP generates an event shortly thereafter on a database server. |
| **Workflow automation** | Workflow defines, executes and automates business processes to pass information or artefacts between actors. This is done so they can execute business processes. Three types of workflows exist, namely, state machine workflow, rules driven workflow and sequential workflow [223]. An example of automated workflow is where a correlation rule triggers the sending of an e-mail |

| SOC Service | Description |
|---|---|
| | to a security administrator, or executes a script that shuts a system down. This is a service that may be offered by the SIEM. |
| **24x7 monitoring** | This service is also sometimes referred to as security information monitoring (SIM), or security event monitoring (SEM). This service collects and analyses information from critical assets identified and rated by the asset management and criticality rating service. The information and events are monitored to detect threats and attacks, allowing actions to be taken on the alerts. In order to be effective, and to provide near real time detection of threats, this service should be offered continuously, twenty-four hours a day, seven days a week. |
| **Forensic analysis** | This service consists of the processes to uncover and interpret digital data. The purpose of this service is to preserve evidence in its original form, while simultaneously following a structured investigative process by collecting, identifying and validating digital information. Past events can then be reconstructed, and used in a court of law, or in other instances [224]. From a SOC, and using a SIEM, fraudulent activities or attacks and, at national level, spying activities by foreign countries may be detected,. |
| **In-house research** | The Merriam-Webster dictionary defines research as "...investigation or experimentation aimed at the discovery and interpretation of facts, revision of accepted theories or laws in the light of new facts, or practical application of such new or revised theories or laws [225]." Cybersecurity research describes research in the cybersecurity domain to find solutions with real-world applications that strengthen national defence, protect the freedom of individuals, and ensures economic resilience and continuity [226]. It is our experience that in-house research refers to an internal organisational service. |
| **Reporting** | Reporting is where a spoken or written account is given on something a person heard, did or investigated It is our experience that reporting on cybersecurity should include an analysis of monitored traffic, external threats and vulnerabilities, remediation's and recommendations. Other than this, reporting often serves as the only way of demonstrating value to clients or organisations. |
| **Vulnerability management** | This service consists of the processes used to identify IT vulnerabilities, and the risks they pose and national or organisational level are evaluated. Based on the evaluation, recommendations can be made, and implemented to correct the vulnerabilities, and removing the risks [227]. Vulnerability management is one of the remediation activities of an overall risk management strategy and process. |
| **Risk management** | This service entails nations applying the principles of risk management to manage IT security risks. it covers all aspects of owning, operating and adapting the use of IT. Risk is defined as the product of the likelihood of occurrence that an event can have on a nation as well as its impact. IT risk is, however, described as the |

| SOC Service | Description |
|---|---|
| | product of the value of the asset, the systems vulnerability to a specific risk, and the threat it poses to the organisation [228]. We have proposed a National Cybersecurity Risk Management Guide in Appendix H. |
| **Network and security device management** | This service manages security technical controls. Management tasks include tasks such as firmware and version updates, operational maintenance, signature updates and configuration. The management of these security technical controls may be done according to an established framework such as ITIL. |
| **Security awareness training** | Security and awareness training may be delivered as part of SOC services. The training may be delivered digitally, as part of induction, or as formal trading sessions. |
| **Consulting** | Clients are consulted on their current security posture and efforts, typically measured against existing standards and frameworks such as ISO/IEC 27001:2013 or NIST SP 800-53. Consultation can range from the configuration of security controls, to solutions and architecture design and business continuity. |

Now that we have identified and consolidated the SOC services, we need to identify and consolidate the CSIRT services. We will do this in In Section D4, where we will pair the SOC and CSIRT services to the E-CMIRC functions (introduced in Appendix C), which is a combination of the SOC and CSIRT functions we have identified in Appendix B and Appendix C. The pairing will be done based on our experience.

## D3 CSIRT cybersecurity services



ENISA [229] and SEI [230] groups the cybersecurity services provided by CSIRTs into three categories, namely, reactive services in the first place – the reactive services are provided in response, or reaction to an incident. Secondly, proactive services consider all cybersecurity services needed for the preparation, protection and securing of systems.Thirdly, security quality management services provide cybersecurity services to enhance existing cybersecurity services. The three cybersecurity categories with their cybersecurity services are listed in Table 41 as described by ENISA [229] and SEI [230].

**Table 41: CSIRT reactive services**

| CSIRT Service | Description |
|---|---|
| **Alerts and warnings** | This service distributes information that describes threats and vulnerabilities such as attacks or viruses. It also makes recommendations to remediate these threats and vulnerabilities. This information may be created by the CSIRT itself, sector-CSIRTs, vendors and security experts, to name a few. |
| **Incident handling** | This service involves "...receiving, triaging, and responding to requests and reports, and analyzing incidents and events." Some of the activities during the response phase can include the taking of remediation actions, issue solutions and |

| CSIRT Service | Description |
|---|---|
| | mitigating strategies, trace intruder activity and recovery. The incident handling service may further be divided into the following categories, and may be offered from different types of CSIRTs.<br>• Incident analysis<br>• Forensic evidence collection<br>• Tracking or tracing<br>• Incident response on site<br>• Incident response support<br>• Incident response coordination |
| **Vulnerability handling** | This service receives hardware and software vulnerability reports. It then analyses the nature, mechanisms and effects of the vulnerabilities, and develop a response strategy to detect and repair them. The following are categories of vulnerability handling services that may be provided by different types of CSIRTs:<br>• Vulnerability analysis<br>• Vulnerability response<br>• Vulnerability response coordination |
| **Artefact handling** | Artefacts are files or objects form a compromised system. These systems may be involved in attacks, or reconnaissance of systems r networks. Some examples of artefacts are Trojans, viruses and worms, and rootkits. This service describes the handling, review and study of these artefacts. The following categories of artefact handling may be offered by different types of CSIRTs:<br>• Artefact analysis<br>• Artefact response<br>• Artefact response coordination |



**Table 42: CSIRT proactive services**

| CSIRT Service | Description |
|---|---|
| **Announcements.** | This service communicates information about threats and vulnerabilities such as intrusion alerts, security advisories and vulnerability warnings to its constituents. The purpose of these announcements is to allow the CSIRT constituents to prepare for, and protect their systems and networks against these threats and vulnerabilities. |
| **Technology watch.** | Technical developments, attack methodologies and intruder developments are monitored to identify future threats. This service may also monitor socio-political threats, as well as the national regulatory and legislative environment. This may be done by subscribing to security mailing lists and websites, as well as current news and articles relevant to the CSIRTs constituency. |

| CSIRT Service | Description |
|---|---|
| **Security audits or assessments.** | This service analyses and review in detail the nation's infrastructure based on the requirements defined in the nation's authoritative and normative sources. It may also review the nation's security practices. Depending on the CSIRT type, the following categories of security announcements or assessments may be offered.<br>• Infrastructure reviews<br>• Best practice reviews<br>• Scanning<br>• Penetration testing<br>It should be noted that scanning and penetration testing forms part of a vulnerability management strategy. Scanning technologies uses signatures and discovers "known" vulnerabilities, while penetration testing discovers "unknown" vulnerabilities. |
| **Configuration and maintenance of tools, applications and infrastructure.** | This service provides guidance, and in some instances perform the secure configuration of systems, and infrastructures of its constituency. The configuration could be on security controls such as intrusion prevention systems (IPSs), firewalls, virtual private networks (VPNs) and authentication mechanisms. |
| **Development of security tools.** | This service develops new cybersecurity tools such as scanners and patches for custom software. It may also include "secure build" images that may be used to rebuild compromised hosts. Tools or scripts extending the functionality of existing tools may also be developed, An example is plug-ins for scanners, and scripts or tools facilitating automated patch distribution. |
| **Intrusion detection services.** | This service reviews logs from its own, or its constituents IPS logs. These logs are analysed, and the CSIRT responds to events that may indicate threats. The IPS signatures are typically configured with thresholds. The CSIRT's response may be governed according to pre-defined service level agreements or operational level agreements. |
| **Security-related information dissemination.** | With this service, a repository of security information is provided to constituents This information should be comprehensive, and readily available. The content may be developed and published by the CSIRT, and may include information from external sources such as sector-CSIRTs, vendors and security experts. Some of the type of information that may be contained in this repository as taken from SEI [230] are:<br>• Reporting guidelines and contact information for the CSIRT.<br>• Archives of alerts, warnings, and other announcements.<br>• Documentation about current best practices.<br>• General computer security guidance.<br>• Policies, procedures, and checklists.<br>• Patch development and distribution information. |

| CSIRT Service | Description |
|---|---|
| | • Vendor links<br>• Current statistics and trends in incident reporting<br>• Other information that can improve overall security practices |

**Table 43: CSIRT security quality management services**

| CSIRT Service | Description |
|---|---|
| **Risk analysis.** | This service augments the risk management analysis strategy and process. It may improve the nation's ability to provide a realistic risk assessment of national cyber assets that are qualified and quantified. This risk analysis is a sub-function of our proposed National Cybersecurity Risk Management Guide we introduced in 0. |
| **Business continuity and disaster recovery planning.** | Security incidents may lead to the disruption or degradation of a nation's services and operations. CSIRTs may provide the business continuity management (BCM) and IT disaster recovery (IT DR) planning service to help with the recovery of national services and cyber operations. This planning may include guidelines on how to respond to national incidents and how to ensure continuity. In our experience, there is a clear distinction between IT DR and BCM in that IT DR only recovers IT systems, while BCM ensures the processes, facilities and people are included in the planning. |
| **Security consulting.** | With this service, CSIRTs advise and guide states on the best practices, at national level, on national cyber operations. This service entails the preparation and compilation of recommendations, as well as identifying functional and technical requirements for the procurement of new systems or security processes. |
| **Awareness building.** | With this service, a CSIRT identifies areas where its constituents require information and guidance to allow them to conform to national authoritative and normative requirements. Creating awareness improves comprehension of security related issues, and allows CSIRT constituents to more securely perform their daily activities. A cybersecurity aware constituency may improve the constituent's chance of detecting attacks and threats, and report on those. Awareness training may be delivered online, using traditional media, and at schools and universities. |
| **Education and training.** | With this service CSIRTs provide security related information regarding cybersecurity issues. This information is delivered via courses, tutorials and workshops. This training may cover all aspects across the project, detect, report, and respond lifecycle of cybersecurity incidents. |
| **Product evaluation or certification.** | With this service, CSIRTs evaluates products, tools, applications or services to ensure their inherent security, and effectiveness and efficiency. These tools may be open source, or commercial off the shelve (COTS). |

## D4 SOC and CSIRT services to E-CMIRC function mapping

We have now introduced the SOC and CSIRT services researched in the authoritative literature. Furthermore, in Chapter 2, we introduced the relationship between cybersecurity functions, services and capabilities, and illustrated the relationship in Figure 9. In addition, we explained that functions are made up of services that consist of capabilities. In turn, capabilities are made up of people, processes and technologies. We also identified SOC and CSIRT functions, and from their functions, made a selection of functions to be included for the E-CMIRC. As a reminder, the E-CMIRC functions are:

- Monitoring and evaluation function.
- Security operations function.
- Threat and vulnerability management function.
- Incident handling function.

We will now draw on our experience in planning, building, running and monitoring SOCs and CSIRTs, to map the E-CMIRC functions to the SOC and CSRIT services we identified in the preceding appendices. Table 40 provided a list of SOC services with a description of each service. Table 41 to introduced the CSIRT proactive, reactive and security quality management services, with a description of each service. The mapping of E-CMIRC functions to SOC and CSIRT services enabling the E-CMIRC functions is displayed in Table 44:

**Table 44: E-CMIRC function to SOC and CSIRT services mapping**

| E-CMIRC Functions | SOC Services | CSIRT Services |
|---|---|---|
| **Monitoring and Evaluation function** | • 24x7 monitoring<br>• Counter intelligence<br>• Surveillance<br>• Risk management<br>• Reporting | • Intrusion detection services. |
| **Security Operations function.** | • Network and Security Device Management<br>• Asset management and criticality rating | • Configuration and maintenance of tools, applications and infrastructure. |
| **Threat and Vulnerability Management function.** | • Aggregation and analysis of intelligence data<br>• Correlation of content intelligence data<br>• Vulnerability management | • Vulnerability handling<br>• Announcements.<br>• Technology watch.<br>• Alerts and warnings |

| E-CMIRC Functions | SOC Services | CSIRT Services |
|---|---|---|
| | • Providing Strategic advice and guidance and Integrated threat intelligence<br>• Reporting | |
| **Incident Handling function.** | • Incident response, incident management<br>• Reporting | • Incident handling |

It is worth mentioning that this mapping is done purely to ensure that all functions are covered by at least one service, or services. This table does not hold the final selection of services for the E-CMIRC. The mapping of the E-CMIRC functions to the SOC and CSIRT services illustrates that there may be instances where the same service can be used to enable more than one function. An example would be the reporting service that may be used as part of the *incident handling* function, as well as the *security operations* function.

We now have a mapping of E-CMIRC functions to SOC and CSIRT services that deliver on them. In Section D5, we will identify similarities and overlaps between the SOC and CSIRT services. This will provide us with a consolidated list of services from which we will make a selection for the E-CMIRC to deliver on its functions.

## D5 SOC and CSIRT cybersecurity service mapping

The mapping of SOC and CSIRT services will assist us with the identification of common and unique services and capabilities. The ENISA grouping of CSIRT cybersecurity services is used as the baseline, as it is a consolidation and good representative of the CSIRT specific services expressed by SANS [198], the SEI at CMU [143], and the International Telecommunications Union (ITU) [231]. The SOC and CSIRT cybersecurity services are grouped as reactive, proactive, and security quality management cybersecurity services to align with the CSIRT service grouping.

Our motivation for selecting the CSIRT services as a baseline is because its services are expressed in international standards and frameworks, while the SOC services are expressed by organisations, and not by any international body, standard or framework.

Table 45 to Table 47 displays the mapping of SOC and CSIRT cybersecurity services. This mapping is done using our experience in planning, building, running and monitoring SOCs and CSIRTs. Table 45 displays the SOC to CSIRT reactive services mapping.

**Table 45: CSIRT to SOC reactive service mapping**

| CSIRT | SOC |
|---|---|
| **Alerts and warnings** | Providing strategic advice and guidance and Integrated threat intelligence |
| **Incident handling** | Incident response, incident management |
| **Vulnerability handling** | Vulnerability management |
| **Artefact handling** | Forensic analysis |

The SOC to CSIRT proactive services mapping is shown in Table 46.

**Table 46: CSIRT to SOC proactive service mapping**

| CSIRT | SOC |
|---|---|
| **Announcements** | • Reporting<br>• Providing strategic advice and guidance and integrated threat intelligence |
| **Technology watch** | • Providing strategic advice and guidance and integrated threat intelligence<br>• In-house research |
| **Security audits or assessments** | Security consulting |
| **Configuration and maintenance of tools, applications and infrastructure** | Network and security device management |
| **Development of security tools** | |
| **Intrusion detection services** | 24x7 monitoring |
| **Security related information dissemination** | • Reporting<br>• Providing strategic advice and guidance and Integrated threat intelligence |

The SOC and CSIRT security quality service management is displayed in Table 47.

**Table 47: CSIRT to SOC security quality management services mapping**

| CSIRT | SOC |
|---|---|
| **Risk analysis** | Risk management |
| **business continuity and disaster recovery planning for constituents** | Security consulting |
| **Security consulting** | Security consulting |
| **Awareness building** | Security awareness training |
| **Education and training** | |

| | |
|---|---|
| **Product evaluation and certification** | Security consulting |

Considering the list of proactive services as mapped in Table 46, the service descriptions by vendors [181], [193], [232] and the definitions of SOCs [233] and CSIRTs [140], it can be inferred that services offered by CSIRTs are mostly focussed outwards, and towards its constituents, while services offered by SOCs are focused internally – in other words, the constituents they reach differ. In addition, the reach differs in that national CSIRTs provide a service to the public as a constituent, while SOCs serve customers, but almost never the public. SOCs do not provide their services at national level, but rather individual organisations, or in the case of MSSPs multiple organisations. The same applies to CSIRTs in terms of serving multiple constituents. Our next step is to identify SOC and CSIRT services that are common, and unique.

Before we continue with the comparison of the SOC and CSIRT services to determine its commonalities and uniqueness, we would like to reinforce what we have done so far to get to the stage where we can compare the services of the two structures. We have started with the identification of SOC and CSIRT cybersecurity functions in Appendices B, and C. From these functions, we have identified and motivated functions for the E-CMIRC. These functions, however, need cybersecurity services to deliver on them (the relationship between functions, services and capabilities were introduced in Chapter 2).

This requirement led us to the identification of SOC services in Section D2, and the CSIRT services in Section D3. We have then mapped the SOC and CSIRT services back to the E-CMIRC functions in Section D4 to ensure that all the E-CMIRC functions are covered by a service. With this mapping, we have seen that there is some overlap and similarity between SOC and CSIRT services.

We will provide a mapping of SOC and CSIRT services in Table 48 to identify SOC and CSIRT commonand unique services. The services of these two structures were identified from authoritative literature sources. Table 48 is a consolidation of the services captured in Table 45 to Table 47, and the mapping is done based on our experience working with SOCs and CSIRTs. This mapping includes the work done by Jacobs *et al.* (2016) [190].

**Table 48: SOC and CSIRT common and unique services**

| CSIRT Unique | Common | SOC Unique |
|---|---|---|
| Development of security tools<br><br>Education and training<br><br>Product evaluation and certification | Alerts and warnings<br>Incident handling<br>Vulnerability handling<br>Artefact handling<br>Announcements<br>Technology watch<br>Security audits or assessments | 24x7 monitoring |

| CSIRT Unique | Common | SOC Unique |
|---|---|---|
| | Configuration and maintenance of tools, applications and infrastructure<br>Intrusion detection services<br>Security related information dissemination<br>Risk analysis<br>Business continuity and disaster recovery Planning for constituents<br>Security consulting<br>Awareness building | |

After analysing the SOC and CSIRT services, we can see that CSIRTs offer the following three unique services:

- Development of security tools.
- Education and training.
- Product evaluation and certification.

When considering the description of the CSIRTs' intrusion detection services described in Table 42, and comparing them to the SOCs' 24x7 monitoring service, it is clear that there is a relationship between the CSIRT intrusion detection service, and the SOCs 24x7 monitoring service. The SOC, with its 24x7 monitoring service, will detect intrusions. No reference to CSIRTs offering 24x7 monitoring as a service could be found in any of the authoritative literature. The SOC specific service we identified is:

- 24x7 Monitoring.



In Table 44, we mapped the E-CMIRC functions to the SOC and CSIRT services, and in the process, made sure that all the E-CMIRC functions have a service, or services associated with them. In Section D4, in Table 48, we compared the SOC and CSIRT services to identify common and unique services. We will now continue with our selection of services for the E-CMIRC. Section D6 introduces all the elements we will consider during the selection process.

## D6 E-CMIRC service selection approach

We have now identified SOC and CSIRT functions, and selected and motivated functions for the E-CMIRC from those functions. We then identified SOC and CSIRT services, and their overlaps and similarities. This left us with the list presented in Table 48 where we have identified the services that are common and unique to SOCs and CSIRTs. We now need to select and motivate services from the list in Table 48 for the E-CMIRC to deliver on its functions. The E-CMIRC services selection is informed by the elements we identified during the

development of the NCMF. The E-CMIRC structure links intimately with the NCMF, and as such, delivers on the authoritative and normative source prescripts, as well as the dimensions, mandates and domains.

It is worth reiterating that the defensive domain lifecycle phases may assist with the identification of national cybersecurity structures as well as the structure's functions and service. This concept was introduced in Chapter 2. Together with the E-CMIRC functions, the defensive domain lifecycle phases will have the biggest influence when selecting services for the E-CMIRC. This is because the defensive domain lifecycle phases are mostly offered from SOCs and CSIRTs, and thus, by definition, the E-CMIRC.

To ensure that the E-CMIRC services are relevant and complete, we will map the SOC and CSIRT services to the defensive domain lifecycle phases of prevent, detect, respond and recover in Section D7. This will provide us with a complete and relevant list of services for the E-CMIRC that deliver on all its functions.

## D7 Selection of E-CMIRC cybersecurity services

We have used the NCMF to identify thirteen of the most general cybersecurity functions, and from those, we have selected and motivated the *monitoring and evaluation* and *incident handling* functions to illustrate the implementation part of the NCMF. We are doing this by developing a new structure called the E-CMIRC. The SOC and CSIRT structures were identified as the structures delivering on the *monitoring and evaluation* and *incident handling* functions. We identified the SOC and CSIRT functions in section D8, and from that list, we have selected and motivated functions for the E-CMIRC.



The SOC services were identified in section D2, and CSIRT functions were identified in section D3. We then mapped the SOC and CSIRT services to the E-CMIRC functions in Table 44 to ensure that all E-CMIRC functions are covered by a service. In Chapter 6, we selected and motivated the critical information infrastructure (CIP) and crisis management mandate to illustrate the application of the NCMF implementation part. The *monitoring and evaluation* and *incident handling* functions deliver on this mandate, and the E-CMIRC functions introduced in Appendix C, section C8, in turn, delivers on the *monitoring and evaluation* and *incident handling* functions.

The dimensions with their actors, as well as the domains and mandates were also introduced in Chapter 3. We also selected the defensive domain as the domain of operation for the E-CMIRC, and introduced the defensive domain lifecycle phases. We now need to ensure that the E-CMIRC services deliver on the defensive domain lifecycle phases.

The defensive domain lifecycle phases were identified in Chapter 3 as protect, detect, respond and recover, and these phases were mapped back to the *Incident Handling* lifecycle. We stated in Chapter 3 that the defensive domain lifecycle phases may assist with the identification of cybersecurity structures and the

services needed for each of its lifecycle phases. The E-CMIRC cybersecurity services firstly have to ensure that they deliver on all the E-CMIRC functions, and this we did in Table 44. Our E-CMIRC must also ensure that the defensive domain lifecycle phases are covered, since it is a structure operating in the defensive domain.

It would thus be helpful if we do a mapping of the E-CMIRC functions and services with regard to the defensive domains lifecycle phases. This ensures that our E-CMIRC functions and their complementary services cover all their lifecycle phases. We will use this section to map the services introduced in Table 44 to the defensive domain lifecycle phases. This mapping then provides us with a list of E-CMIRC services. During the development of the NCMF level 1 in Chapter 2, we recommended that the selection and prioritisation of national cybersecurity functions should follow a risk-based approach. During the identification of the thirteen general cybersecurity functions in Chapter 4, we introduced the *national strategic risk and threat assessment* function. This function resides at level 2 of the NCMF, and is one of the thirteen general cybersecurity functions.

In order to comply with the recommendation of following a risk-based approach to assist in the identification of national cybersecurity functions and services, the risk analysis service is selected to be a fundamental part of the E-CMIRC services. The full complement of services we need to make a selection from for the E-CMIRC is listed below, as taken from Table 44 and as supported by previous research done by Jacobs *et al.* (2016) [190]. This list contains the SOC and CSIRT unique and common services as presented in Table 48:

- Risk analysis.
- Development of security tools.
- Education and training.
- Product evaluation and certification.
- Alerts and warnings.
- Incident handling.
- Vulnerability handling.
- Artefact handling.
- Announcements.
- Technology watch.
- Security audits or assessments.
- Configuration and maintenance of tools, applications and infrastructure.
- Intrusion detection services.
- Security related information dissemination.
- Business continuity and Disaster recovery planning for constituents.
- Security consulting.
- Awareness building.
- 24x7 monitoring.

This list includes the services needed to deliver on the E-CMIRC functions as shown in our mapping of E-CMIRC functions to SOC and CSIRT services in Table 44. Our list of services however consists of more services than those needed to deliver on the E-CMIRC functions. To exclude some of the additional services to be offered from the E-CMIRC, we will do a mapping of our list of services to the defensive domain lifecycle phases.

We will first map all services delivering on the E-CMIRC functions. It makes sense that the services not needed to deliver on the E-CMIRC functions, or the defensive domain lifecycles are excluded. Doing this mapping provides us with a list of E-CMIRC services that are relevant and complete in terms of being able to deliver on the crisis management mandate, E-CMIRC functions, and also the defensive domain lifecycle phases. The services are mapped back to the E-CMIRC functions and the defence domain lifecycle phases in Table 49, and this mapping is done based on our experience. We will populate Table 49 with the services we have presented in Table 48. We will use the following abbreviations for the functions make the table more readable:

- Monitoring and evaluation function - ***ME***
- Security operations function - ***SO***
- Threat and vulnerability management function - ***TVM***
- Incident handling function - ***IH***

**Table 49: Services mapped to E-CMIRC functions and defensive domain lifecycle phases**

| | Protect | Detect | Respond | Recover |
|---|---|---|---|---|
| **ME** | | 24x7 monitoring<br>Intrusion detection services | | |
| **SO** | | Risk analysis<br>reporting | Network and security device management | Business continuity and disaster recovery planning |
| **TVM** | Vulnerability management | Alerts and warnings | Security related information dissemination | |
| **IH** | | | Incident handling | |

Table 49 contains the mapping of services across the E-CMIRC functions and the defensive domain lifecycle phases. This mapping was done based on our experience, and keeping in mind the *monitoring and evaluation*, and *incident handling* national functions. This means that we have not considered services such as asset management and criticality rating, and security audits or assessments or consulting, as they fall outside the scope of the *monitoring and evaluation*, and *incident handling* functions. We only considered services relevant to the *monitoring and evaluation*, and *incident handling* functions.

Some services, such as the business continuity and disaster recovery planning fall outside the national scope, and it is our experience that this service is something that is delivered at organisational, or critical infrastructure level. We have however included this service as it is the only SOC and CSIRT service addressing the recovery lifecycle phase. We envision that the E-CMIRC will fulfil an overseeing and advisory role with regard to this service. The list of services we have thus identified and selected to be offered by the E-CMIRC is:

- 24x7 monitoring
- Intrusion detection services
- Risk analysis
- Reporting
- Network and security device management
- Business continuity and disaster recovery planning
- Vulnerability management
- Alerts and warnings
- Security related information dissemination
- Incident handling

Most of these services that we have mapped, may overlap the E-CMIRC functions and defensive domain lifecycle phases. An example is the vulnerability management service that is grouped under the *threat and vulnerability management* function and the protect lifecycle phase, but this service may also be found as part of the *security operations* function in the respond phase.



There are various standards, frameworks and best practices that may be consulted when considering incident handling, security related information dissemination, and situational awareness at national level [143], [126], [149], [234], national cybersecurity risk management [235], [236], [10] and business continuity and disaster recovery [237], [238], [239].

We could, however, not find any publicly available sources on how to implement the monitoring and intrusion detection and prevention service at national level. In section D8, we will make a proposition on how to achieve monitoring and intrusion prevention at national level. This is important since 24x7 monitoring and intrusion detection are two critical services we propose for the E-CMIRC.

## D8 Monitoring and intrusion detection at national level

While incident handling at national level is common, and copious reference literature, frameworks, best practices and successful reference implementations exist, it is our experience that the same cannot be said

for monitoring, and intrusion detection and prevention at national level. This section explains how monitoring of the national cyber domain may be achieved to detect events that may lead to national cybersecurity incidents. Our purpose is not to go into technical details, but to propose a high-level national monitoring service with current existing technologies and their capacity to show that it is possible to have a monitoring function at national level.

Some examples of countries with successful implementations of national CSIRTs offering the national *incident handling* function, are countries such as the United States of America, Belgium and South Korea [240] [241]. The ITU reports that there are currently 103 national CSIRTs in existence [242]. The ITU's list of existing national CSIRTs may be accessed at https://goo.gl/dRgktU .

Monitoring the national cyber environment to detect attacks, and responding to those attacks, is one of the functions that the E-CMIRC structure will offer. Some characteristics of national cyber-attacks are that they could originate from various actors and sources, be aimed at national cyber assets, could affect more than one organisation or sector within an industry, and may have effects identical to kinetic attacks. [1]. The national cyber-attack characteristics are repeated in the UK's Cyber Security Strategy document [243].

In an environment where cybersecurity technical controls are monitored (such as a SOC with a SIEM tool), events and alerts are received form the technical controls by the SIEM. Based on a machine or human analysis, some of these events or alerts may then be classified as an incident. It is necessary to monitor these events to detect attacks.

The monitoring of technical controls forms the tenet or basis by which cybersecurity events and alerts are detected, and classified as incidents. Once an incident occurs, it must be responded to. The scenario we have just described, the monitoring of security technical controls, the classification of the technical control's events and alerts as incidents, and the response thereto, typically occurs at organisational level.

It is our experience that monitoring and detection at national level is not done commonly. Our experience has shown that one of the reasons that nation states do not monitor technical controls at national level, is that products are not available that can handle the bandwidth capacity at national level, and neither are there national structures from where monitoring and detection of attacks can be done at national level. Nation states use a distributed CSIRT model, relying on sector-CSIRTs to detect, and report on attacks.

It must again be noted that we previously stated in Appendix C that no authoritative literature source listed monitoring as a CSIRT service. In terms of monitoring at national level, events across all national ingress points into a country could be monitored. South Africa, as an example of a developing country, has five active cable systems connecting South Africa to the world [244] [245]. These systems and the bandwidth they provide are shown in Table 50.

**Table 50: South African active cabling systems [182] [183]**

| System Name | Bandwidth |
|---|---|
| South Atlantic 2 (SAT-2) | 560 Mbits/s |
| South Atlantic 3 / West Africa submarine cable / South Africa far east (SAT-3 / WASC / SAFE) | 340 Gbits/s |
| SEACOM | 2.6 Tbits/s |
| East African submarine cable system (EASSy) | 4.72 Tbits/s |
| West African cable system (WACS) | 5.12 Tbits/s |

The bandwidth from these systems is then distributed inland to three Internet Exchange Points (INX). There is an INX in each of the South African largest economic centers. These INXs are being run and operated by Internet Exchange South Africa (INX-ZA), which is an sovereign division of the Internet Service Providers Association (ISPA) [246]. The three inland INXs are situated at Johannesburg (JINX), Cape Town (CINX), and Durban (DINX) with Johannesburg and Cape Town being multi sites [247]. JINXS provides 8 Gbits/s and CINX provides 3 Gbits/s [248], while DINX provides 2 Gbits/s throughput [249].

It is proposed that the ingress points in developing countries be protected using IPSs. Protection can be extended to provide firewalling service, as well as a national DDoS shelter. There are currently carrier-class technologies available providing IPS throughputs of up to 30 Gbits/s [250]. This would satisfy the 8 Gbits/s throughput at JINX, which is the highest throughput provided across all three INX's. This strategy is applied successfully in South Korea [251]. We further proposed that these IPSs then be monitored from an E-CMIRC-like structure. This allows for a monitoring and detection service at national level.



## D9 Conclusion

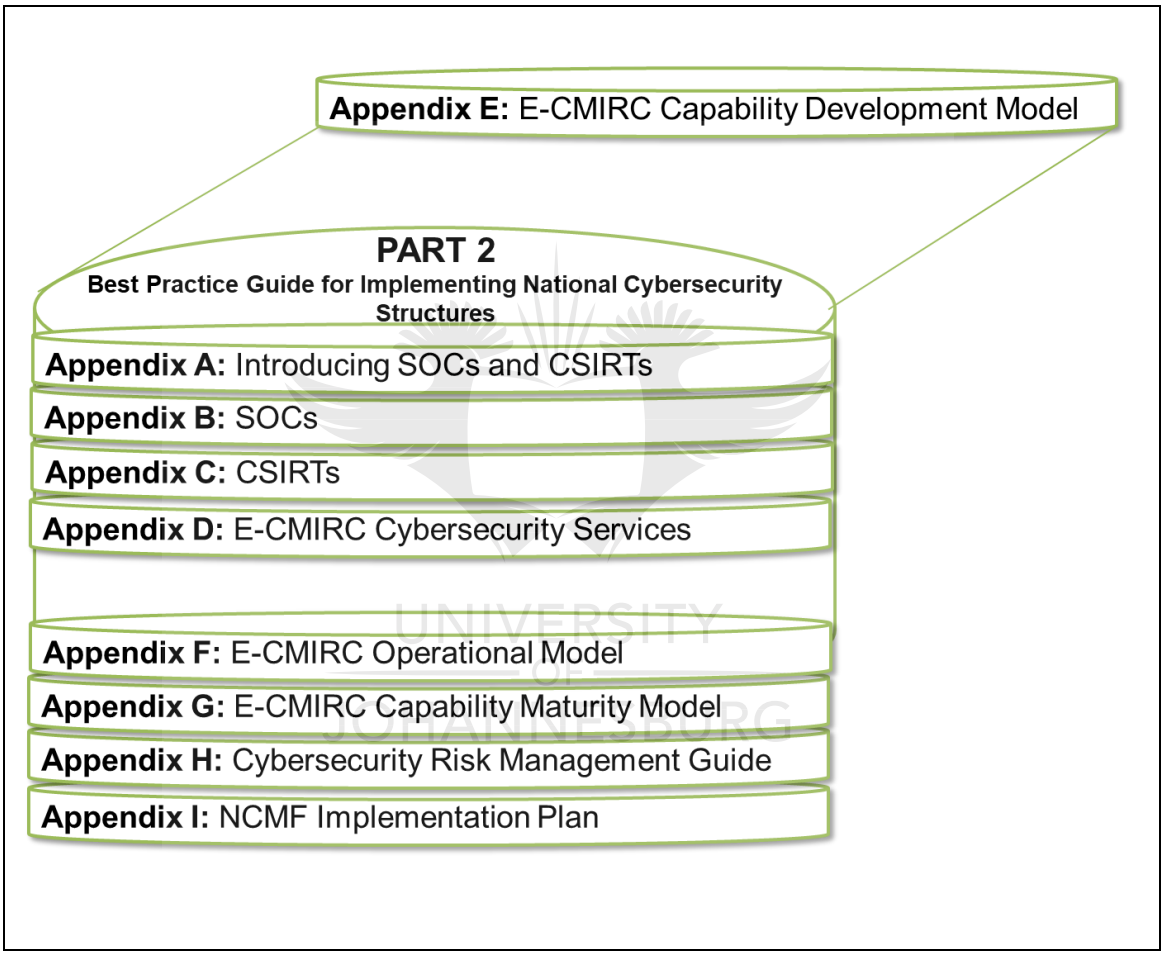
The purpose of Appendix D was to identify and select the E-CMIRC services. The SOC and CSIRT services were determined in Section D2 and Section D3. We used the following approach to help us during the identification and selection of the E-CMIRC services:

- We identified SOC services from authoritative literature in Section D2.
- We identified CSIRT services from authoritative literature in Section D3.
- We then mapped the SOC and CSIRT services to the E-CMIRC functions (identified in Appendix C) in Section D3. Doing this gave us certainty that all E-CMIRC functions are covered by a service, or more than one service.
- We identified common and unique SOC and CSIRT services in Section D6. This gave us a list of common and unique SOC and CSIRT services.

- This list of common and unique SOC and CSIRT services were then mapped to the E-CMIRC functions, and the defensive domain lifecycle phases in Section D7. This provided us with a list of services for the E-CMIRC.

An approach to monitoring and protecting national ingress points were presented in Section D8. In Appendix E to Appendix F we will introduce the E-CMIRC structure, and its representative models. The. E-CMIRC structure is described using three models, the E-CMIRC CDM, the E-CMIRC OM and the E-CMIRC MM.

Using the NCMF, we have identified thirteen of the most general cybersecurity functions, and we have selected two of those as functions for our E-CMIRC. We have identified the existing structures of the two selected functions to be used as a reference during the development of our E-CMIRC. The two existing structures are SOCs and CSIRTs and we then identified the SOC and CSIRT functions, and selected and motivated SOC and CSIRT functions for the E-CMIRC. Following the selection of functions, we then identified the services needed to deliver on those functions, and made a selection from them for the E-CMIRC. In Appendices E to F, we will describe the "**b**uild," "**r**un" and "**m**onitor" functions of the **PBMR** organisational approach.


Appendix E: E-CMIRC Capability Development Model
PART 2
Best Practice Guide for Implementing National Cybersecurity Structures
Appendix A: Introducing SOCs and CSIRTs
Appendix B: SOCs
Appendix C: CSIRTs
Appendix D: E-CMIRC Cybersecurity Services
Appendix F: E-CMIRC Operational Model
Appendix G: E-CMIRC Capability Maturity Model
Appendix H: Cybersecurity Risk Management Guide
Appendix I: NCMF Implementation Plan

# Appendix E: E-CMIRC capability development model (E-CMIRC CDM)

## E1 Introduction

We have introduced the E-CMIRC functions in Appendix C, and the E-CMIRC services in Appendix D In this Appendix, we will develop a generic model that may be used as a reference model when developing the E-CMIRC capabilities. The focus of this appendix is thus to develop the E-CMIRC capability development model (E-CMIRC CDM). Our model will be based on existing capability development models. The approach we will follow is to develop the E-CMIRC CDM is as follows:

- We will identify and analyse existing capability development models.
- An existing capability development model will be identified and selected to be used during the development of our E-CMIRC CDM.

The E-CMIRC CDM will be combined with the E-CMIRC operations model (E-CMIRC OM) and presented as a single, integrated model in Appendix F. We are doing this since there is a correlation and overlap between the E-CMIRC capabilities and the E-CMIRC operations in that every aspect or element making up the capability development model, has to be considered during each operational element.

The rest of this appendix is structured as follows:

**Section E2** presents the E-CMIRC in context of the NCMF. Our aim is to illustrate where the E-CMIRC fits within the NCMF.

**Section E3** Introduces capability models and describes the value they offer during the development of a system.

**Section E4** is used to introduce publicly available capability development models, and we will select a capability development model for the E-CMIRC.

**Section E5** describes the capability model that we have selected for the E-CMIRC.

**Section E6** concludes this appendix.

## E2 E-CMIRC structure in the context of the NCMF

To identify national cybersecurity functions, we have proposed a framework that may be used to identify cybersecurity functions needed at national level. We introduced this framework, the NCMF, in Chapter 3 and Chapter 5 (Chapter 4 was used to identify the most general non-mandatory cybersecurity functions). The NCMF provides developing countries with a framework to identify, select, prioritise and implement national cybersecurity functions.

During the identification of the general cybersecurity functions in Chapter 4, the *monitoring and evaluation*, and *incident handling* functions from the National Crisis Management mandate, residing in the defensive domain, were selected to illustrate the implementation part of the NCMF. Keeping in the fiscal and skills constraints of developing countries in mind, we have motivated the delivery of the cybersecurity services on these two functions (traditionally offered from two different structures – the SOC and CSIRT) combined, and offered from a new, single structure, the E-CMIRC.

The NCMF national cybersecurity function *identification* part starts at level 1 and the *selection* and *prioritisation* of functions are done at level 2. The NCMF cybersecurity function *implementation* part starts at level 3 and ends at level 6. Our E-CMIRC is a newly envisioned, national cybersecurity structure that offers the combined services of the *monitoring and evaluation*, and *incident handling* functions.



All national structures, inclusive of the E-CMIRC, reside at level 3 of the NCMF. The E-CMIRC structure, as a national cybersecurity structure, will also have authoritative, normative source prescripts. These prescripts will influence the building, running and monitoring requirements of the structure. Some of the national structures used by the United States of America are the cyber security coordinator (CSC), the United States Computer emergency readiness teams (US-CERT) and the industrial control systems cyber emergency response team (ICS-CERT) [68]. Some examples of national cybersecurity structures in the United Kingdom, are the Office of Cyber Security and Information Assurance (OCSIA), the Cyber Security Operations Centre (CSOC) and the Computer Emergency Response Team (CERT-UK) [68].

In using South Africa as a sample developing country, structures mandated by the NCPF [33] and the South African Cybercrimes and Cybersecurity Bill [34] are the Government CSIRT (ECS-CSIRT) [83], the Cybersecurity Hub [82] serving as the national CSIRT, the Department of Defence's Cyber Command, and the South African Police's Cybercrimes Centre. The E-CMIRC

structure, represented by the cube, in the context of the NCMF is shown in Figure 39 that depicts that the E-CMIRC structure resides at level 3 of the NCMF, and that it requires the elements captured in levels 5 and 6 of the NCMF.

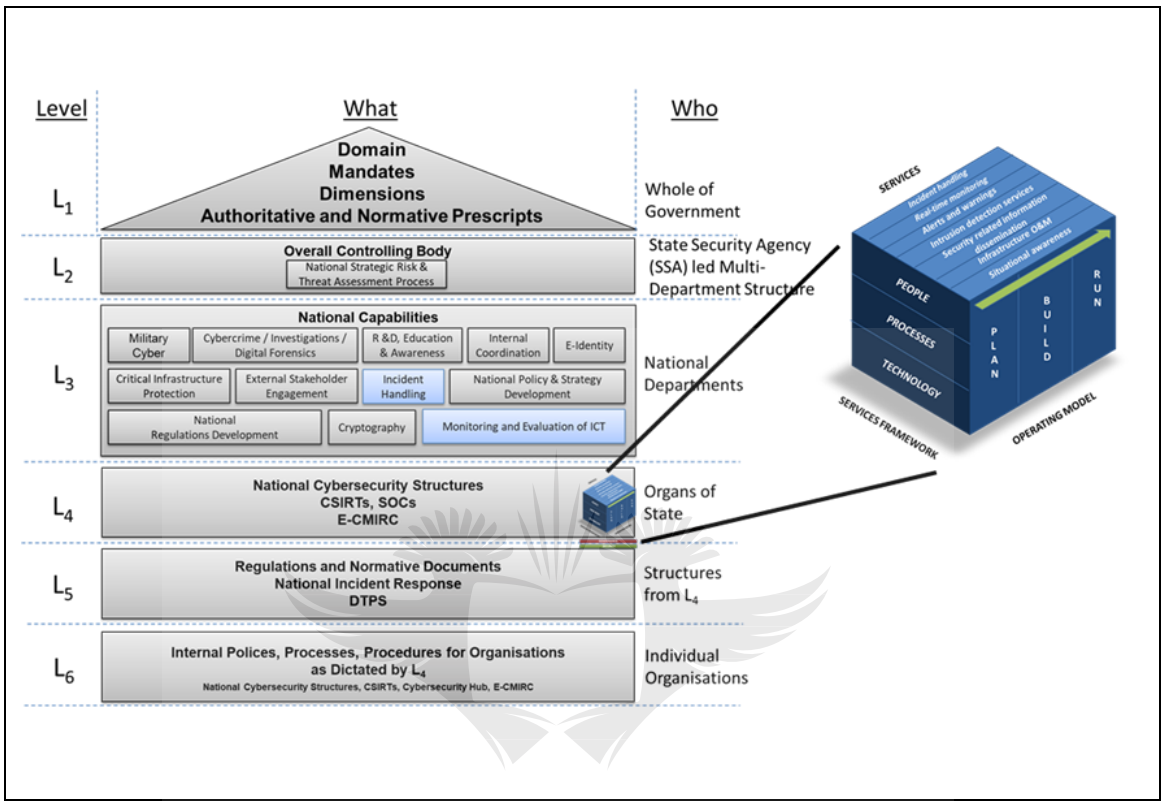



**Figure 39: Position of E-CMIRC in the context of the NCMF**



The E-CMIRC CDM describes what the E-CMIRC's capabilities should look like, keeping in consideration its people, processes and technologies. Levels 5 and 6 of the NCMF serves to guide the national structures through identifying applicable legal and regulatory requirements, and policies, processes and procedures needed to comply to these requirements, as well as policies, processes and procedures needed to deliver on its services and operations.

## E3 Introduction to capability development models

The Merriam-Webster dictionary defines the concept of a 'model' as *"a description or analogy used to help visualize something (as an atom) that cannot be directly observed"* [252]. The E-CMIRC will be described using a model. The E-CMIRC capability development model will be an abstract, visual model. The value that a model can provide in representing a system is as follows [253]:

- It allows for the documentation of E-CMIRC requirements and functions.

- Enables assessment of the performance of the E-CMIRC structure.
- Enables cost estimation.
- Allows for the evaluation of trade-offs.
- Aids in performance management, decreases risk and manages cost.

The E-CMIRC is a structure, much like a SOC or CSIRT. Considering the value that following a model may offer during the planning and building of structures, it would be helpful if there were a model that nations can follow during the planning and building of the E-CMIRC's capabilities. Following a capability development model allows the E-CMIRC structure to be broken down into its components. It also serves as a blueprint to assist those building the structure to make sure that all components are considered and catered for [254].

## E4 Existing capability development models

The E-CMIRC's cybersecurity services are made up of capabilities, and these in turn consist of people, processes and tools or technologies in turn (this was described in Chapter 2). We have made a conscious decision to only consider the capability development models of military systems, and our motivation is as follows:

- Our research did not produce any existing *cybersecurity* capability development models or frameworks.
- Teoh (2010) [255] proposed a cybersecurity capability process that describes practices. This is not relevant as a reference framework.
- Our research returned *system* capability development frameworks, and of those, the military system capability development frameworks were found to be the most comprehensive and complete.
- In Section 1.10 we have recommended that national cybersecurity structures should be planned and built as systems, and according to systems engineering principles. In keeping with our recommendation, we will thus only consider system capability development models.
- Our E-CMIRC serves at national level, and may be used to offer functions across the Offensive or defensive domains. Although the E-CMIRC development is illustrated in context of the defensive domain, our intention is also for a nation state to be able to use it to deliver functions in the offensive domain. In our discussion on domains in Section 0, we stated that functions in the offensive domain are often military functions, and this resonates with our alignment with military capability development models.

The capabilities of South African defence systems are described in a granular fashion [256], and can be seen to cover aspects of personnel, organisation, sustainment, training, equipment,

doctrine, facilities, information, technology and budget (POSTEDFIT-B) [257] [258]. The POSTEDFIT-B capability development model is used in South Africa, by the South African DOD for the development of military systems. Other available military capability development models are training, equipment, personnel, infrastructure, doctrine and concepts, organisation, information, logistics (TEPID-OIL) used by the UK Ministry of Defence [259]. The United States (US) Department of Defence (DOD) uses doctrine, organisations, training, materiel, leadership, personnel and facilities (DOTMLF) [260]. These capability development models are the smallest dimensions of the people, processes and technology or tools framework [261].

The POSTEDFIT-B, TEPID-OIL and DOTMLF are all military capability development models. Military capability development models are a comprehensive way of defining work deliverables and work standards, and they provide a way to measure the work deliverables [262]. In Chapter 2 we have described a service as consisting of a capability, or capabilities. The E-CMIRC structure offer functions and services to deliver on the monitoring and evaluation, and incident handling functions. Furthermore, by definition, the E-CMIRC structure is an information communication and technology (ICT) related structure, and at its core, ICT service delivery, has people, processes and technology [190] [263].

## E5 E-CMIRC capability development model selection

We have selected the POSTEDFIT-B as the most ideal capability development model for the E-CMIRC as it is the most comprehensive model when comparing it against the other available military capability development models. It also has a proven track record. An example of where it was applied successfully in a developing country, is with the development of the South African armoured capability [258].

We found it to have a wider coverage and is more modular when compared against the UK MOD and the US DOD capability development models. Another motivational factor is that the other military capability development models are developed for, and used by developed countries, and the POSTEDFIT-B model is used by a developing country.

A further advantage of the POSTEDFIT-B's granularity, is that trade-offs can be made between the model's elements. This allows for the optimisation of the E-CMIRC, and allows us to compensate for deficiencies in individual elements [257]. A comparative analysis between the UK MoD and US DoD capability development models against the POSTEDFIT-B model is made in Table 51.

**Table 51: Comparison of capability development models**

| POSTEDFIT-B | TEPID-OIL | DOTMLF |
|---|---|---|
| Personnel | Personnel | Leadership |
| Organisation | Organisation | Organisation |
| Sustainment | Logistics | x |
| Training | Training | Training |
| Equipment | Equipment | Materiel |
| Doctrine | Doctrine and concepts | Doctrine |
| Facilities | Infrastructure | Facilities |
| Information | Information | x |
| Technology | x | x |
| Budget | x | x |

The second column in Table 51 shows that the UK Ministry of Defence's TEPID-OIL model does not describe technological or budgetary requirements, and the third column shows that the US DOD's DOTMLF models does not cover sustainment, information, technology or budget. The absent elements are indicated with an "x."

Table 51 makes it clear that the South African military's South African POSTEDFIT-B capability development model is the most comprehensive and granular model. We will now provide a description of each of the elements making up the POSTEDFIT-B capability development model, and contextualise it for our E-CMIRC.

## Personnel

In the POSTEDFIT-B model, personnel describes the required characteristics of the people elements [264] staffing the E-CMIRC. In staffing the E-CMIRC, the Skills Framework for the Information Age (SFIA) [64] may be considered as a framework that describes the skills needed within the E-CMIRC, while the National Initiative for Cybersecurity Education (NICE) National Cybersecurity Workforce Framework [265] could be considered to organise, describe and label cybersecurity work. Mandatory South African human resource (HR) requirements and conditions of employment for staff working in our E-CMIRC may be found in acts such as the Basic Conditions of Employment Amendment Act No 11 of 2002 [266].

## Organisation

This capability development element describes the organisational structure of the E-CMIRC. In the South African context, and following the NCMF levels, the organisation of the E-CMIRC may be constructed from the actors identified using the proposed stakeholders and actor identification template we introduced in Section 3.5 in Chapter 3. We have also expressed the requirement of an

overall controlling body in Section 5.4. The overall controlling body may be a body similar to the Cyber Response Committee [120] and the National Cybersecurity Advisory Council [121] introduced in Section 5.4.

The responsibility of the overall controlling body would be to determine the E-CMIRC organisational structure. It is proposed that the E-CMIRC be organised according to its constituents, the reason being that different skills would be needed for different constituents. The skills required to perform the *monitoring and evaluation* and *incident handling* functions for CI, that typically uses programmable logical controllers (PLC's) and supervisory control and data acquisition (SCADA) systems, differ from the skills needed to support *monitoring and evaluation* and *incident handling* functions for the financial sector, or normal data networks.

The E-CMIRC may also be structured across geographic locations, service domains, or across business units. An example of a business unit-oriented structure, is the fact that the South African government consists of different departments such as the Department of Justice (DOJ), The Department of Home Affairs (DHA), and the Department of Defence (DOD), and the E-CMIRC may be structured accordingly. A sample organisational structure is shown in Figure 40.

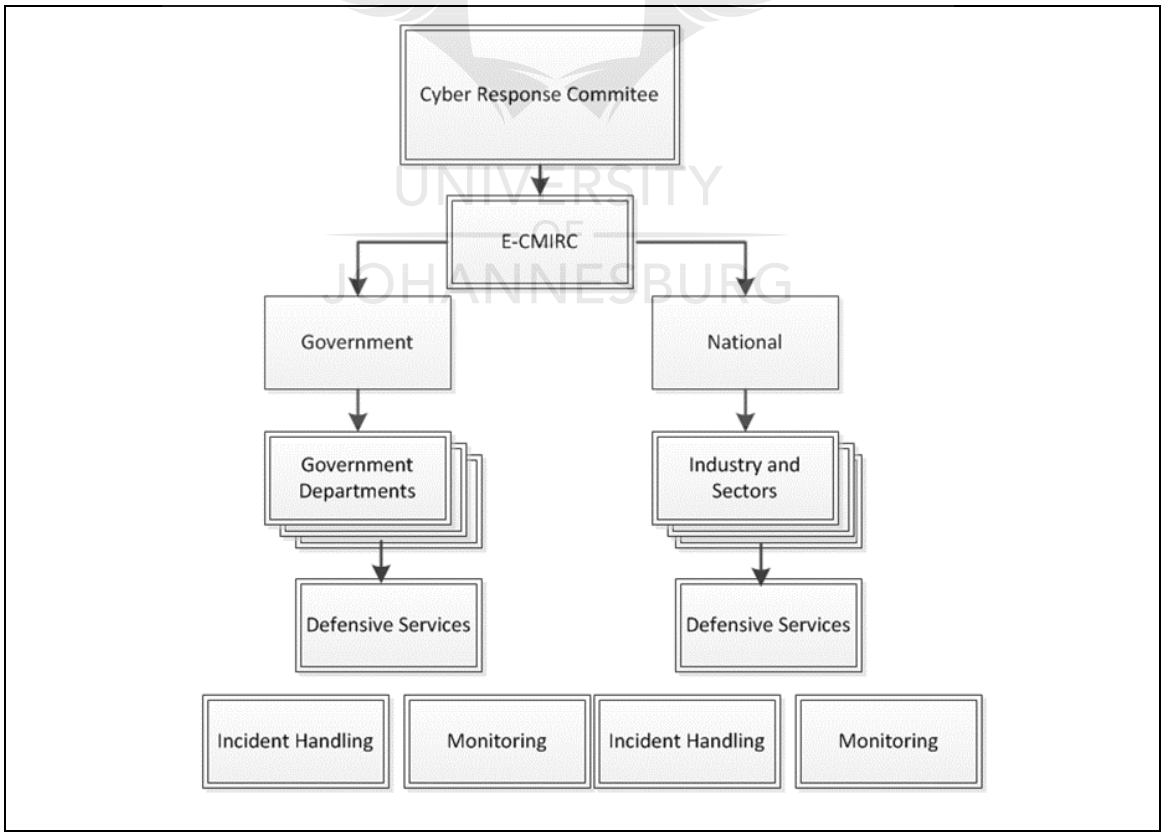



**Figure 40: Sample E-CMIRC organisational structure**

In this sample organogram, an overall controlling body as specified in level 2 of the NCMF, will have control over the E-CMIRC structure. The E-CMIRC itself is structured to provide services to government, and at national level in the defensive domain. This defensive services layer is purposefully inserted to illustrate the flexibility of the E-CMIRC - should the E-CMIRC mature, and national cybersecurity functional requirements change, it would be easy to add services applicable to the offensive domain, such as a cyber warfare service.

The focus of the E-CMIRC is to provide a *monitoring and evaluation* and *incident handling* function at national level, but any of the thirteen identified general cybersecurity functions identified in Chapter 4 may be added, omitted, or nation state specific national cybersecurity functions added, as the E-CMIRC structure matures, and as national requirements change.

## Sustainment

In the POSTEDFIT-B model, sustainment describes support elements such as financial, logistics and personnel support [264]. This element is also known as supply and support [267]. In context of the E-CMIRC structure, this element refers to the provisioning of technology, tools and assets the E-CMIRC requires to start and continue its operations, as well as the management of its configuration, serviceability and availability. It includes aspects such as financial and HR support. The technology, tools and assets are discussed later in this Section and include elements such as a SIEM tool, and a help desk system.



## Training

This element refers to the training for the E-CMIRC staff that is needed. Training requirements need to be defined. The defined training should include aspects such as how frequent training will take place, the depth and breadth of required skills and competence needed, and also whether certification training should be considered. It should be kept in mind that training should be split into technical or technology specific training, as well as service specific training such as incident handling, and monitoring and analysis training. Legal and management training should also be provided. In the identification of skills and required training, frameworks such as SFIA [64] and NICE [265], as introduced in Section 3.5.4 may be considered.

## Equipment

This POSTEDFIT-B element describes the supporting equipment needed for the E-CMIRC to perform on its operational mandate. Equipment include elements such as chairs and tables, office and stationary equipment, an equipped pause area, monitoring screens, an equipped visitors area,

and a war room to name a few. A requirements analysis may be performed to identify all the equipment needed.

### Doctrine

This element describes the management, control, policy, strategy and regulatory framework of the E-CMIRC. This correlates with levels five and six of the NCMF, and governs administration, operations and decision making in the E-CMIRC. This element may include sources such as national policy, an example is the NCPF, down to technology specific processes and procedures, such as a back-up process and procedure. The policies and processes will be developed taking into consideration the mandate of the E-CMIRC, and its service offering to stakeholders.

## Facilities

In the POSTEDFIT-B model, facilities refer to the physical structure itself, the building and property. The facility should be chosen in such a way that it supports the operation of the E-CMIRC. From a South African context, the building location may be sited in an area where both municipal and national power grids are available to ensure redundancy. The building should also conform to physical security requirements such as those expressed by the SAPS minimum physical security standards (MPSS) [268], or ISO/IEC 27001:2005 [48].

## Information

This POSTEDFIT-B element describes all information input and output. It covers aspects such as cyber intelligence data and its processing systems, the format of presented information or cyber intelligence, its timelines and reliability and correlation. The E-CMIRC will use various information streams as input, such as the IPS events, and threat intelligence and incidents from stakeholders and third parties. It is our experience that these elements are mostly technology dependant, and this should be kept in mind when conducting a technology requirements analysis.

## Technology

This element describes the technology and tool requirements for the E-CMIRC to perform its mandate. Some of the tools that may be needed in the E-CMIRC, are:

- SIEM Tool.
- Threat intelligence / business intelligence tool.

- Supporting services such as terminal servers, file servers, DNS servers, mail server, a public key infrastructure and NTP server.
- Carrier-class intrusion prevention systems.
- Screens, and workstations.

From a South African context, the tool functional and technical requirements may be identified by following a systems engineering (SE) approach. This entails a user requirement analysis, a functional requirements specification and a technical requirements specification. These specifications should be coupled to measures of effectiveness (MoE's), and measures of performance (MoP's). In South Africa, from a Department of Defence perspective, the SE process is governed by the defence acquisition policy (DAP) 1000 based on SE principles [269]. Staying within the context of South Africa, the acquisition of these technologies and tools, will have to conform to the Public Finance Management Act of 2012 (PFMA Act) [270] if the acquisition is facilitated by state owned companies or government departments.

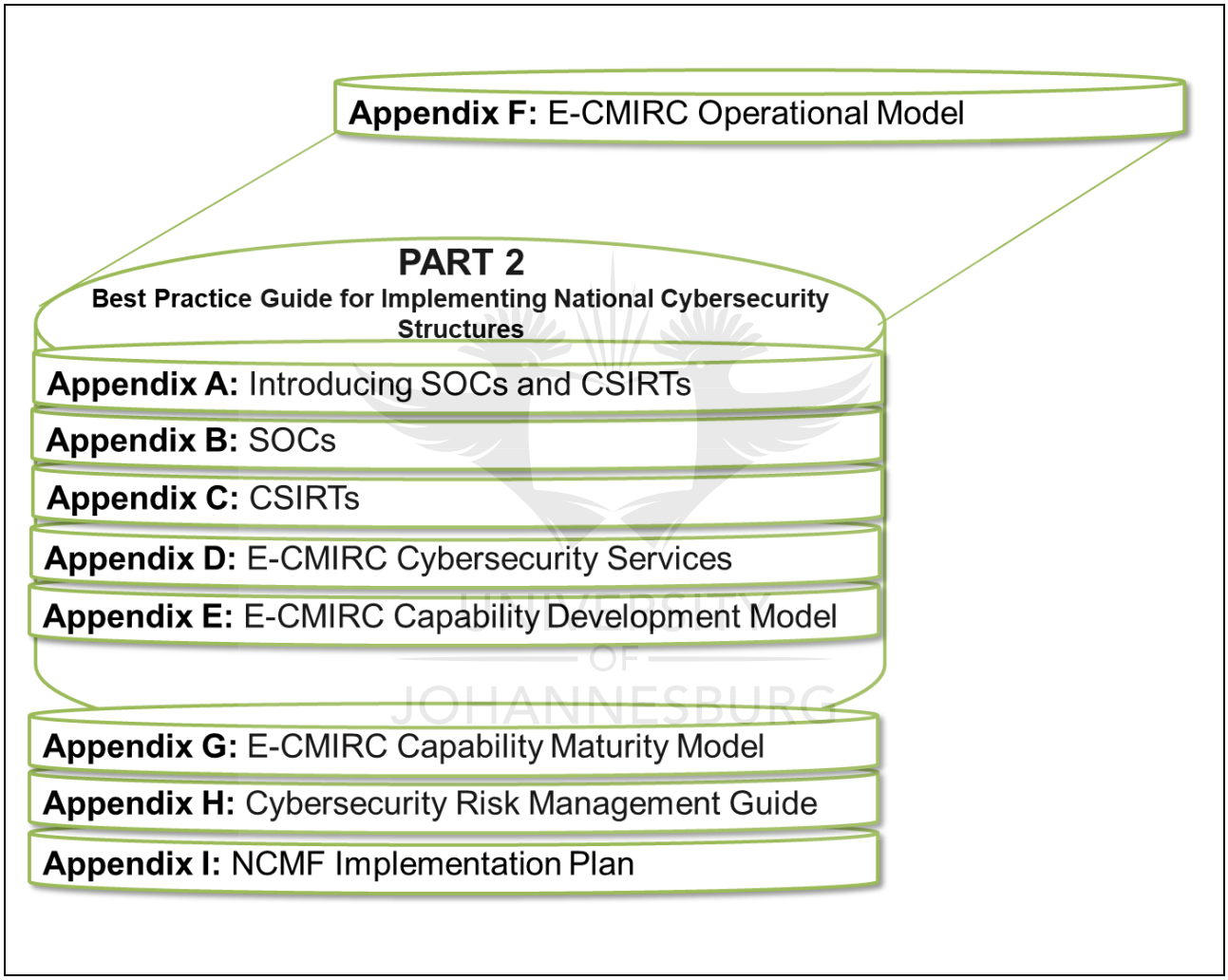
### Budget

This element describes the budgetary requirements. It also addresses the financial model by which the E-CMIRC will operate, as well as from where funding will be sourced. This is a political decision. To govern financial expenditure, acts such as the PFMA is used, as well as regulations and guidelines from National Treasury.



## E6 Conclusion

In this Chapter, the POSTEDFIT-B capability development model was selected and motivated for use in the development of the E-CMIRC capability development model. Our motivation for selecting the POSTEDFIT-B model, is that it is the most complete and granular capability development, and its use is proven in a developing country. We provided a description of each of the POSTEDFIT-B elements, and explained its use in terms of the E-CMIRC. In Appendix F we will be developing the E-CMIRC operations model. The E-CMIRC CDM and the ECMIRC OM will be represented in a single, integrated model.


Appendix F: E-CMIRC Operational Model
PART 2
Best Practice Guide for Implementing National Cybersecurity Structures
Appendix A: Introducing SOCs and CSIRTs
Appendix B: SOCs
Appendix C: CSIRTs
Appendix D: E-CMIRC Cybersecurity Services
Appendix E: E-CMIRC Capability Development Model
Appendix G: E-CMIRC Capability Maturity Model
Appendix H: Cybersecurity Risk Management Guide
Appendix I: NCMF Implementation Plan

# Appendix F: E-CMIRC Operational Model (E-CMIRC OM)

## F1 Introduction

In Appendix F we will develop the E-CMIRC operations model (OM). The approach that we will follow is to first identify and analyse existing operations models. From the identified and analysed operations models, we will select one most suitable for the E-CMIRC, and motivate its use. We will then represent the E-CMIRC CDM and the E-CMIRC OM as a single, integrated model. This model may then be used to guide and steer nation states when building an E-CMIRC structure. The rest of the appendix is structured as follows:

**Section F1** introduces existing operational models.

**Section F2** selects and motivates an operational model for the E-CMIRC.

**Section F3** Presents the E-CMIRC CDM and E-CMIRC OM integrated model.

**Section F4** concludes this appendix.

In Section F2 we will be presenting existing operations models.

## F2 Existing operational models



We will first define what an operating model is. An operating model is a visual or abstract representation of how customers derive value, or benefits from an organisation. It further describes the way an organisation does business. It is not static, and continuously undergoes change [271]. At its core, operating models prescribes where and how work gets done across an organisation, or capability. Operating models link organisational strategy and organisational design to deliver on organisational strategy [272].

Research done by Ross, Weill and Robertson (2006) has shown that operational efficiency is 31% higher in organisations with operating models, and has a 33% higher customer satisfaction rating. Organisations with operating models has a 34% advantage during the development of new product and services over their competitors [273]. There thus exists a clear benefit for the E-CMIRC to be gained by using an operating model.

Different ways of defining the elements out of which an operating model exists, are possible. One of the most common ways of defining operating models is the people, processes and technology framework [274]. Another way of defining operating models, is using the process, organisation and technology framework [275]. There are many industry standard operating models such as the:

- TM Forum's Enhanced Telecom Operations Map (eTOM), Business Process Framework [276] founded in 1988 [277].
- Insurance Application Architecture (IAA) [278]
- The Banking Industry Architecture Network (BIAN) [279],
- Information Framework (IFW) [280],
- ITIL [157].
- COBIT [281].

In 2014, KPMG proposed a next generation IT operating model, consisting of the broker, integrate and orchestrate IT, operating model [282], while Cognizant formulated an IT operations model in 2016 with organisation and structure, process, technology and tools and workforce and sourcing as core tenets [283].

We have selected the TM Forum's eTOM Business Process framework as an ideal framework to build the E-CMIRC OM. The motivation for selecting the TM Forum's eTOM Business Process framework is that we have proposed its use for building SOCs in previous work [19]. It is able to scale to national level, it is a comprehensive business process framework, and it is relevant for an IT service capability [19]. For these reasons, the eTOM Business Process framework is chosen as the operating model for the E-CMIRC. The TM Forum's eTOM framework is discussed in Section F3.

## F3 E-CMIRC operating model selection

TM Forum has over 900-member companies, and is globally the largest trade association. They seek to integrate digital ecosystems. Some examples of the digital ecosystems are enterprises, communication service providers, and digital service providers. TM Forum has created a set of standards and best practices in the operationalisation of capabilities which is accepted by over 900 globally dispersed organisations and commercial entities. Businesses globally review, test and validate these standards and best practices [284]

The TM Forum consist of four frameworks. They are the Business Process Framework (eTOM), the Information Framework (SID), the Application Framework (TNA) and an Integration Framework (TAM). The frameworks are collectively known as the New Generation Operation Systems and Software (NGOSS) [285]. The four NGOSS frameworks are shown in Figure 41.

The eTOM Framework is a complete framework addressing marketing and sales, strategy, infrastructure and product, as well as operations and enterprise management [280] [286]. It considers all aspects of business, and categorizes all business activities [286]. Milham (2004) [287], states that one of the advantages of the eTOM Framework is that it establishes a prevalent vocabulary for business processes as well as functional processes. For the purpose of developing the E-CMIRC operations model, the eTOM Business Process Framework will be used as taken from [284]:

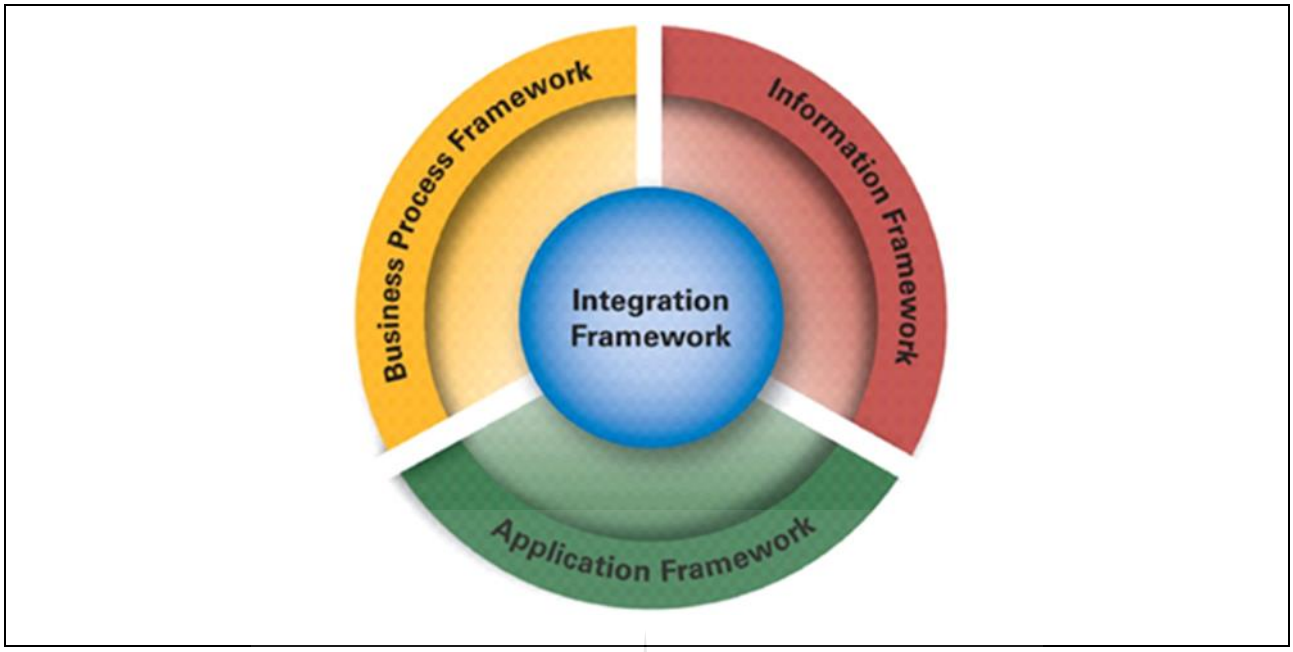



**Figure 41: The four NGOSS frameworks** [284]

The eTOM Business Process Framework is selected as it is the most applicable model for managing operations that uses defined processes. TAM provides a model for how business capabilities are deployed using applications [288], and SID defines information flows through organisations and their service providers [289]. The Integration Framework provides a standard for the integration of management applications and platform services [290]. None of these frameworks, however, provides an operational model and business process descriptions, except eTOM.



The eTOM Framework branches into three business concepts, called levels. The first levels are called level 0, and they are strategy, infrastructure and product (Level 0), operations (level 0) and enterprise management (level 0). [284]. The horizontal layers are level 1 processes A description of each is listed below [19],[291]:

- Strategic, infrastructure and product level - includes marketing and offer management, service management, management resource development and supply chain development. None of these elements are addressed by any of the existing operations frameworks such as COBIT or ITIL. Vertically, this level has the following child-levels:
  - Strategy and commit
  - Infrastructure lifecycle management
  - Product lifecycle management.

  Horizontally, this level has the following child-levels
  - Marketing and offer management
  - Service development management

- Resource development management
- Supply chain development management

- Operations - includes customer relationship management. In contexts of the E-CMIRC, these would be the stakeholders and actors defined in Chapter 2, resource management, operations management and supplier / partner relationships. Vertically, this level has the following child-levels:
  - Operations support and readiness
  - Fulfilment
  - Assurance
  - Billing and revenue management

  The following child-levels are found in the horizontal layer
  - Customer relationship management
  - Service management and operations
  - Resource management and operations
  - Supplier / partner relationship management

- Enterprise Management - this level addresses strategic and enterprise management, risk management, enterprise effectiveness management, knowledge and research management and financial and asset management. Enterprise Management has as child-levels the following:
  - Strategic and enterprise planning
  - Enterprise risk management
  - Enterprise effectiveness management
  - Knowledge and research management
  - Financial and asset management
  - Stakeholder and external relations management
  - Human resources management



The eTOM framework with its horizontal and vertical child-levels are shown in Figure 42. The eTOM framework is comprehensive, and the model drills down to four child levels [19]. During the development of the E-CMIRC model, the capability development framework (POSTEDFIT-B) was motivated for use, and the TM Forum's eTOM framework was selected and motivated for the operations model. The selection of applicable elements from the POSTEDFIT-B framework and the eTOM framework would differ from country to country.

The intention is for the country implementing the cybersecurity service of E-CMIRC structures to select the appropriate elements from the eTOM Framework based on the authoritative, normative, and regulatory prescripts, and also considering the dimensions, mandates and domains.

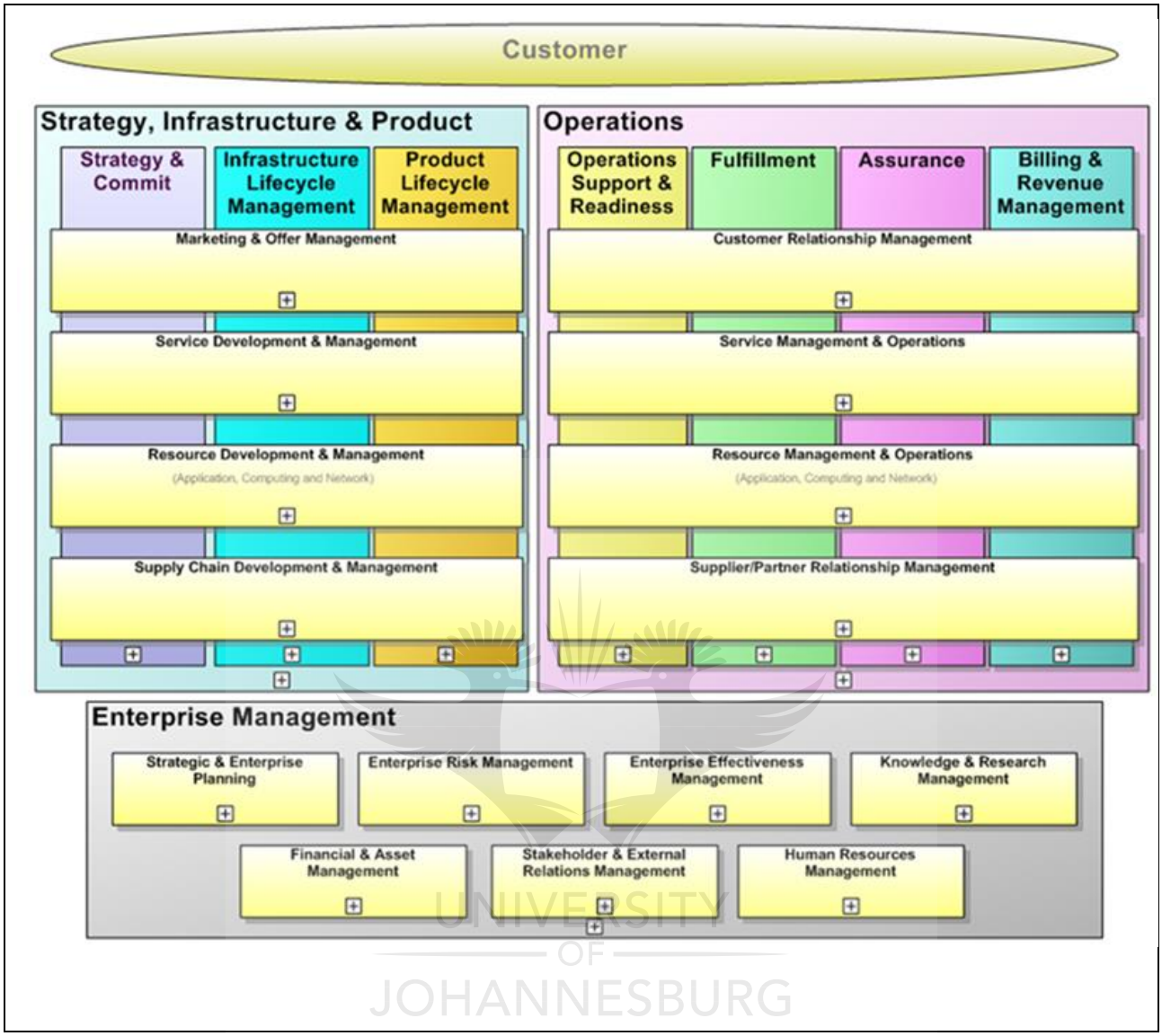





**Figure 42: eTOM framework with horizontal and vertical child levels**

## F4 Presentation of the E-CMIRC CDM and OM

Our NCMF provides us with a framework to assist with the identification cybersecurity functions. It also provides us with a framework to be used during the implementation of national cybersecurity functions. Our NCMF was shown to be flexible enough to be applied to organisations and enterprises, and at national level.

The E-CMIRC, as a national cybersecurity structure that offers cybersecurity functions, must comply with prescripts expressed in authoritative, normative and regulatory documents. The structure's capabilities must consider all elements that may influence its effectiveness, efficiency and costing. To help with this, we have proposed the E-CMIRC CDM. We have selected the POSTEDFIT-B model used by the South African DOD for

developing E-CMIRC capabilities. Our decision was motivated by the fact that the model's application and success is proven in the context of a developing country, and it was also found that it is more comprehensive than its international counter parts.

The E-CMIRC CDM ensures that all the elements making up the E-CMIRC services' complementary capabilities are considered. Following our E-CMIRC CDM helps to guide costing, and allows for repeatable and consistent results during the development of capabilities for our E-CMIRC. To achieve proper governance and management of the operational aspects of the E-CMIRC capabilities, we propose the E-CMIRC OM. Every single capability has operational aspects coupled to it. This means that the capabilities and operations are integrated and tightly linked. There thus exists a relationship between the E-CMIRC CDM, and the E-CMIRC OM.

The E-CMIRC cybersecurity services were selected in Section D4. The complementary capabilities of these services will be developed using the E-CMIRC CDM, and the capabilities' operational aspects will be governed by the E-CMIRC OM. The services we have selected for the E-CMIRC are:

- 24x7 monitoring
- Intrusion detection services
- Risk analysis
- Reporting
- Network and security device management
- Business continuity and disaster recovery planning
- Vulnerability management
- Alerts and warnings
- Security related information dissemination
- Incident handling



The E-CMIRC CDM and OM model is presented in Figure 43. The E-CMIRC model is presented as a symbolic model in the shape of a three-dimensional cube. The first or upper side of the cube covers the cybersecurity services selected in Appendix D. The second side of the cube represents the selected operating model, which is the TM Forums eTOM framework with levels strategy, infrastructure and product, operations and enterprise management. The intention is for the nation-state applying the E-CMIRC OM model to develop the E-CMIRC structure, to drill down to all four levels of the framework, and to identify the applicable eTOM framework business processes based on the national cybersecurity functions they have selected.

The third side of the cube represents the selected capability development model, which, in the case of the E-CMIRC, is the POSTEDFIT-B framework. The intention is for the entity developing the E-CMIRC to use the POSTEDFIT-B framework to ensure that all aspects are considered during the capability development cycle.

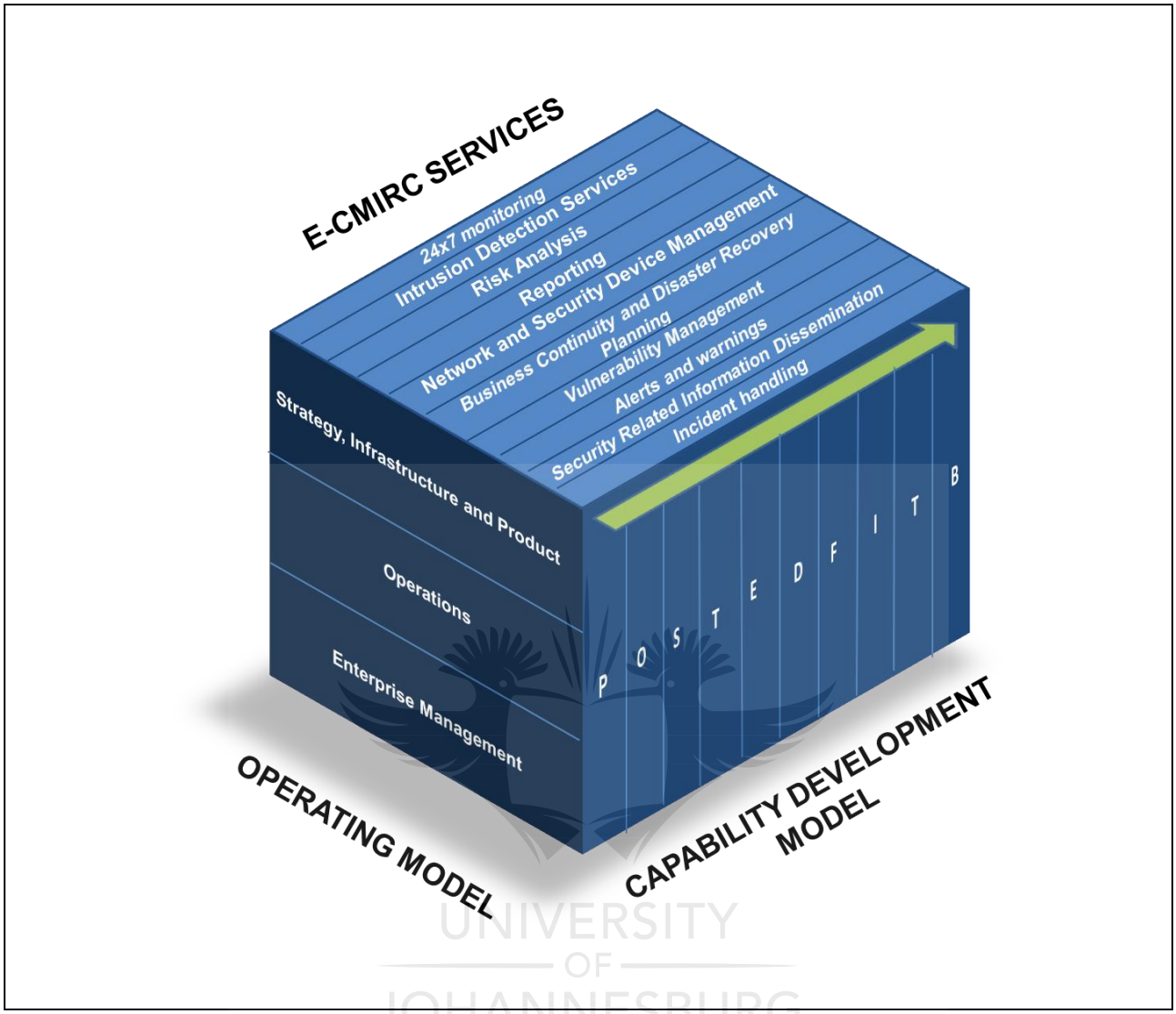




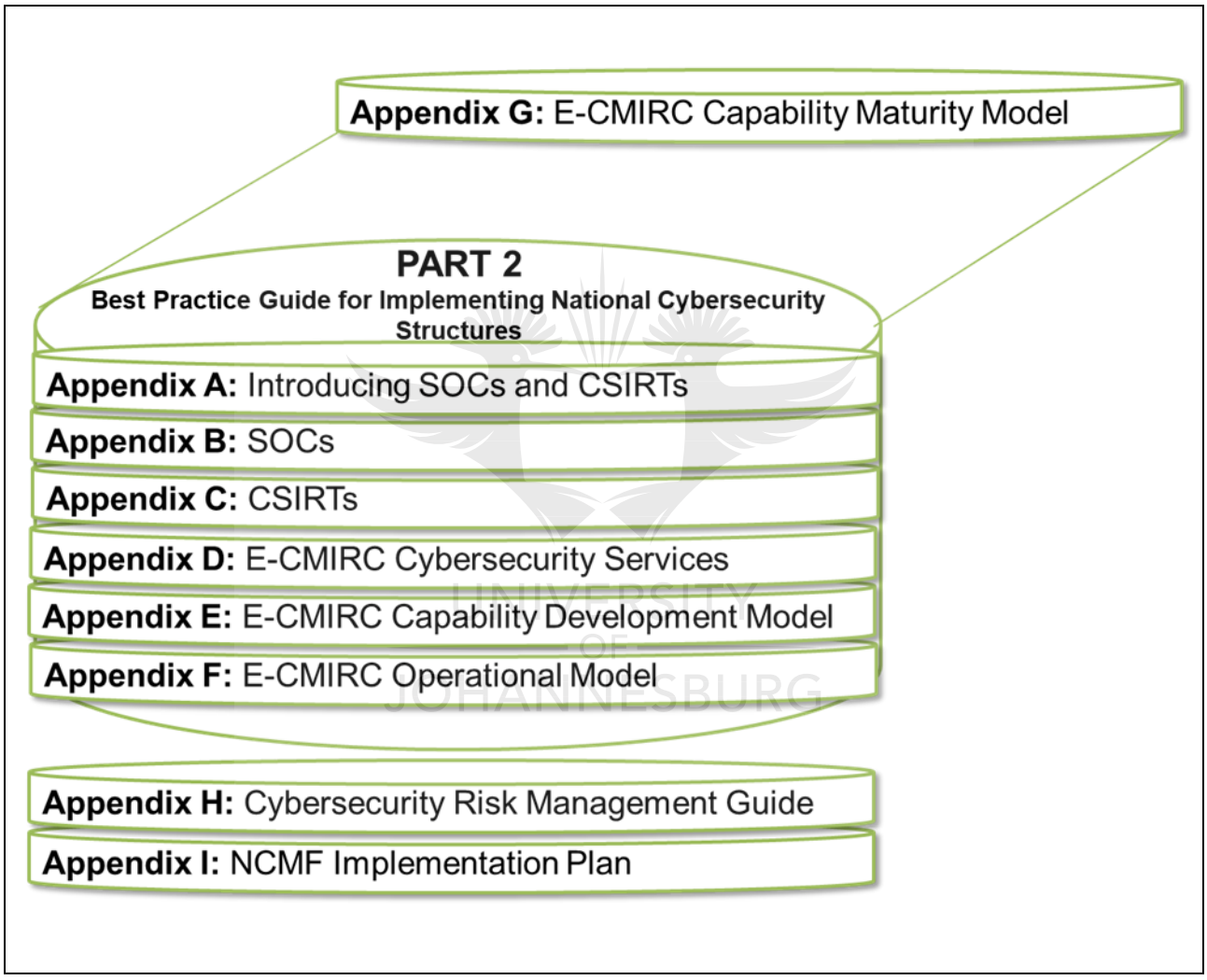

**Figure 43: E-CMIRC CDM and OM model**

This granular approach allows for trade-offs to be made between the framework elements to optimise the E-CMIRC, or to compensate for deficiencies in individual elements [257]. Figure 43 further shows that for each of the services capabilities, the POSTEDFIT-B model should be followed during the development of the capability. For example, the incident handling capability will be developed following the POSTEDFIT-B capability development model. Once the capability is developed and implemented, the eTOM model describes its operational aspects.

## F5 Conclusion

In the preceding chapters, we developed the NCMF to help with the *identification, selection* and *prioritisation* of national cybersecurity functions. These tasks are achieved in the first two levels of the NCMF. The

*identification, selection and prioritisation* tasks satisfy the **p**lan function of the **PBRM** organisational approach, which is the overall organisational framework we have selected. The *implementation* task is illustrated by the development of the E-CIRC, a structure that is described using three models. The E-CMIRC CDM, the E-CMIRC OM and the E-CMIRC CMM. The E-CMIRC CDM satisfies the **b**uild function of the **PBRM** approach, while the E-CMIRC OM satisfies the **r**un function of the **PBRM** organisational approach. To comply with, and complete the **PBRM** organisational approach, the **PBRM m**onitor function needs to be described. To satisfy this function, we will develop the capability maturity model for the E-CMIRC, the E-CMIRC CMM in Appendix G.


Appendix G: E-CMIRC Capability Maturity Model
PART 2
Best Practice Guide for Implementing National Cybersecurity Structures
Appendix A: Introducing SOCs and CSIRTs
Appendix B: SOCs
Appendix C: CSIRTs
Appendix D: E-CMIRC Cybersecurity Services
Appendix E: E-CMIRC Capability Development Model
Appendix F: E-CMIRC Operational Model
Appendix H: Cybersecurity Risk Management Guide
Appendix I: NCMF Implementation Plan

# Appendix G: E-CMIRC Capability Maturity Model (E-CMIRC CMM)

## G1 Introduction

The focus of this appendix is on the development of a model that can be used to measure and manage the effectiveness and efficiency of the E-CMIRC structure's capabilities. In Chapter 2, we showed that capabilities are made up of people, processes, and technology, and that these are housed in, and offered from a structure. The E-CMIRC structure's capabilities and operations are described by the E-CMIRC CDM and E-CMIRC OM. These two models were presented in a single integrated model since the E-CMIRC services (and its complementary capabilities) are linked to its operations.

Now that there is a model to guide and steer the E-CMIRC services' complementary capabilities, and operations, we need a mechanism to baseline, measure and improve the E-CMIRC structure's capabilities. The E-CMIRC CMM provides a mechanism to measure, monitor and manage the E-CMIRC structure, capabilities' effectiveness and efficiency. We will be spending more time on the development of our E-CMIRC CMM. Our rationale for doing so is as follows:

- Having a capability maturity model available during the early phases of the NCMF implementation, allows for the early assessment of existing structures. This early assessment may assist when having to make a decision on whether a new structure is needed for the national cybersecurity functions, or whether an existing structure will suffice.
- A capability maturity model may assist with assessments during the implementation phase of national structures. Based on the outcomes, corrections and adjustments to the structure capabilities may be made early in the development of the structure.
- Having a maturity model available early on may shape structure implementation requirements. To illustrate this, if we know beforehand that we need an incident handling capability with a high maturity level, we can start recruiting people with the right skills and experience, and procure the most relevant technologies.

The rest of this appendix is structured as follows:

**Section G2** introduces the concept of capability maturity models.

**Section G3** introduces the approach we will follow for the development of the CMM.

**Section G4** introduces some of the publicly available capability maturity models, and here we select and motivate a publicly available capability maturity model for the E-CMIRC.

**Section G5** introduces the process maturity assessment criteria.

**Section G6** introduces the technology maturity assessment criteria.

**Section G7** presents the E-CMIRC CMM.

**Section G8** concludes the appendix.

We will now, in Section G2, introduce and discuss the concept of maturity models.

## G2 Introduction to maturity models

Using a capability maturity model will allow for capability elements (people, processes and technology) to be baselined, assessed and improved. It also provides a mechanism to measure the effectiveness and efficiency of capabilities. In context of the E-CMIRC, the assessment would be the responsibility of the national cybersecurity structure management team (E-CMIRC management), and they may report their findings into the overall controlling body we have introduced in Chapter 5.

The capability maturity model will further allows management to assess its processes and methods according to best practices, or against external standards [292]. Capability maturity models may be used to assess the following capability elements:



- People performance
- Processes
- Technology.

A well-developed capability maturity model can also asses structures [293]. These are all the elements that makes up a capability as explained in Chapter 2. The advantages of having a maturity model to measure the E-CMIRC capabilities against, is that a baseline, or benchmark can be easily established, leading to repeatable results when building multiple national cybersecurity structures.

A capability maturity model also allows for the determination of an “as-is” and “to-be” states, and provides guidance on how to improve the maturity of capability elements. Our intention is to design the maturity model flexible enough to cater for all envisioned applications of the E-CMIRC, such as where the E-CMIRC functions, mandates and domains change. Some advantages to using a capability maturity model are [294]:

- It can be used as a benchmark to compare the current state of capabilities
- It provides a model to ensure repeatable results and outcomes when building national

cybersecurity structures.

- It allows for the representation of the progression of capabilities
- It assists in the identification of capability strong and weak points

When designing a capability maturity model, there are two methods the designer can follow. Following the first method as proposed by Becker, Knackstedt and Pöppelbuß (2009) [295], the designer would follow a top-down approach, and start by specifying a fixed number of maturity levels.

These stages are then substantiated with characteristics that could serve as assessment items. The second method as proposed by Lahrmann, Marx, Mettler, Winter and Wortmann (2011) [296] follows a bottom-up approach, in that characteristics and assessment items are first specified, and then grouped into maturity levels.

The E-CMIRC capability maturity model (E-CMIRC CMM) will be designed using the top-down approach as proposed by Becker *et al.* [295]. This is an intentional decision since there are many existing, established and proven capability maturity models using the top-down approach such as:

- Cybersecurity Capability Maturity Model (C2M2) [294].
- Building Security In Maturity Model (BSIMM) [297].
- Systems Security Engineering Capability Maturity Model (SSE-CMM) [298].
- Software Assurance Maturity Model (openSAMM) [299].
- ITIL Maturity Model [300].
- COBIT Maturity Model [301].



The existing capability maturity models are explored in the next section, and an existing capability maturity model is identified to serve as the basis for the design of the E-CMIRC Capability Maturity Model. Our approach to developing the E-CMIRC CMM is introduced in Section G3.

## G3 Our E-CMIRC CMM development approach

In Figure 9, in Chapter 2, we introduced the concept that' services fulfil a function.' We further illustrated that a service is made up of capabilities, and these in turn consist of people, processes and technology. During the development of the E-CMIRC, the following concepts need to be understood, and kept in mind. The first concept we would like to introduce is the concept of 'capability elements.' When we refer to the term "capability elements," we refer to the granular elements making up a capability. These are the people, processes and technology that makes up a capability. The maturity of these elements is something that can be assessed and measured.

The second concept is one of a 'capability maturity score.' This is typically a numeric value. The maturity score may be anything from a maturity score of 0, to a maturity score of 5. The maturity score typically works on a sliding scale, with a score of 0 indicating a low, or bad maturity level, and a score of 5 indicating a high, or good maturity level. Most publicly available frameworks and standards' maturity scores use a similar approach. We will explore the available maturity frameworks in Section G4.

The third concept we would like to introduce, is that entailing maturity assessment criteria. The maturity assessment criteria describe the capability element being assessed, and is linked to the maturity score. It would typically describe that a maturity score of "0" means that the capability element under assessment is non-existent, poorly managed, or needs improvement. It may describe a maturity score of "5" as optimised, well managed, or advanced. The concepts we have introduced are displayed in Figure 44.

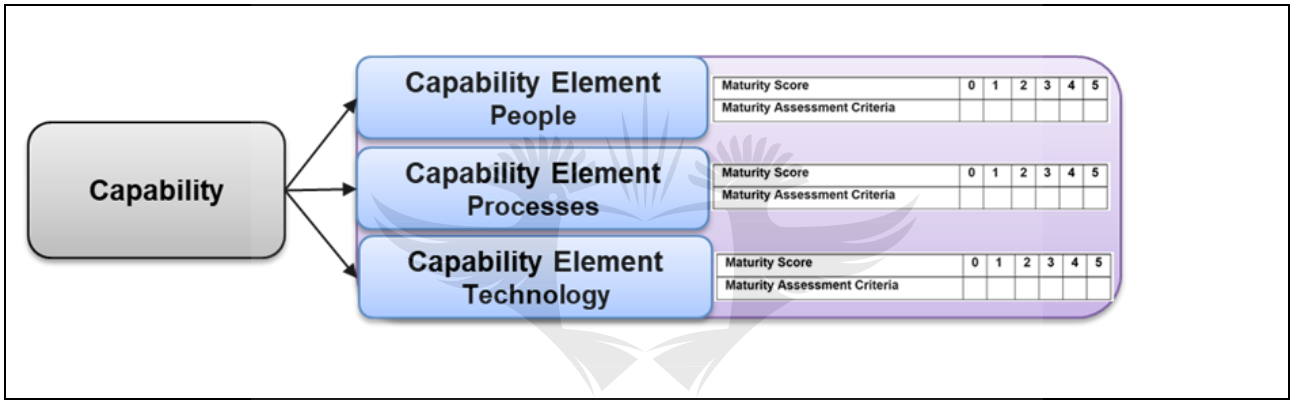



**Figure 44: E-CMIRC CMM concepts**



Figure 44 shows the now familiar concept that a capability consists of people, processes and technology. We have decided to call these capability elements. Each capability element is assessed against a specific assessment criteria, and is scored by a maturity score. During the development of our E-CMIRC CMM, and in keeping with our decision in Appendix E to follow a top-down approach, we will do the following:

**Step 1:** As a first step, we will research, and review existing capability maturity models. Our focus will be on identifying a maturity score numeric value, as well as the maturity assessment criteria that will be scored against the maturity score.

**Step 2:** Throughout this thesis we have mentioned that our intention is to combine the processes and technologies of different functions to realise a cost and skills saving. In keeping with our intention, we will thus determine maturity assessment criteria for E-CMIRC processes and technologies, and exclude the people and structure capability elements. Our intention is not to provide comprehensive maturity assessment criteria for all capability elements.

Our intention is to illustrate how to use our E-CMIRC CMM. The maturity assessment criteria will differ from country to country, and from capability to capability. We will illustrate the application of the E-CMIRC with a maturity assessment criteria example in Section G5. Maturity assessment criteria need to be developed for all the capability elements under assessment. To assist with the compilation of assessment criteria, international standards and frameworks such as ISO/IEC 27001:2013 [128], COBIT 5 [302] and ITIL [303] may be consulted.

In Section G4 we will introduce existing capability maturity models. We are exploring these so we can discover and select a maturity level numeric value, and maturity assessment criteria for our E-CMIRC processes.

## G4 Existing capability maturity models

In order to develop a capability maturity model for the E-CMIRC, and as a first step, some existing capability maturity models will be considered, and the most applicable existing model will be selected and motivated for our E-CMIRC CMM. We will then use the maturity score and the maturity assessment criteria of the selected model as maturity scores and criteria for our E-CMIRC processes. As a second step, the assessment criteria to be used for the technology capability element assessment will be introduced.

From a cybersecurity perspective, three capability maturity models stand out as they address cybersecurity capabilities at national level, and were developed, in some instances, as part of national initiatives. These cybersecurity capability maturity models are:

- The Cybersecurity Capability Maturity Model (UK CMM V 1.2) developed by the Cyber Security Capacity Center in 2014 sponsored by the UK government to be used by the UK government and other governments [53].
- The Cybersecurity Capability Maturity Model (US-C2M2) developed in 2014 by the US Department of Energy for the electricity sub-sector. In version 1, all sector specific references and terminology were removed to make it applicable to all industries and sectors at national level. It was then called C2M2 [294].
- The Systems Security Engineering Capability Maturity Model (SSE-CMM) developed in 1998 and reviewed in 2014 by the International Systems Security Engineering Association (ISSEA). This resulted in an international standard, ISO/IEC 21827:2008 [304]. The aim of the standard is to describe the characteristics needed in organisational or departmental engineering process to ensure effective security engineering [305]. The standard covers the following, as taken verbatim from [305] in order not to detract from the standard's intention and meaning:

    - The entire life cycle, including development, operation, maintenance and decommissioning activities;
    - The whole organization, including management, organizational and engineering activities;

- Concurrent interactions with other disciplines, such as system, software, hardware, human factors and test engineering; system management, operation and maintenance;
- Interactions with other organizations, including acquisition, system management, certification, accreditation and evaluation.

The three capability maturity models with their maturity scores, and the process maturity assessment criteria are compared in Table 52.

**Table 52: Maturity model levels and level descriptions [31], [230], [239]**

| Numeric Score | UK CMM V 1.2 Numeric level description | US-C2M2 Numeric level description | SSE-CMM Numeric level description |
|---|---|---|---|
| **0** | **Start-up** | Non-existent | Not performed |
| **1** | **Formative** | Initial practices are performed but may be ad hoc | Performed informally |
| **2** | **Established** | Practices are documented.<br>Stakeholders of the practice are identified and involved<br>Adequate resources are provided to support the process (people, funding, and tools).<br>Standards and/or guidelines have been identified to guide the implementation of the practices. | Planned and tracked |
| **3** | **Strategic** | Activities are guided by policies (or other organisational directives) and governance.<br>Policies include compliance requirements for specified standards and/or guidelines.<br>Activities are periodically reviewed to ensure they conform to policy.<br>Responsibility and authority for performing the practices are assigned to personnel.<br>Personnel performing the practices have adequate skills and knowledge. | Well-defined |
| **4** | **Dynamic** | | Quantitatively controlled |
| **5** | **Continuously improving** | | Continuously improving |

The first column describes the maturity score's numeric value. This value may be provided by the designer of the maturity model, or the maturity score values may be selected from existing models. We have decided to

use the COBIT maturity level numeric values. The values ranges from “0”, indicating that a process is non-existent, to “5” indicating a mature, and optimised process [302]. ITIL also uses numeric maturity levels, starting at “1” indicating an initial maturity level, to “6,” indicating an optimised maturity level. Since the E-CMIRC is a start-up structure, it will happen that capability elements are non-existent, and we need to be able to indicate this. We thus resonate with the COBIT maturity score numerical value that indicates a score of “0,” or a “non-existent” capability. In Section G5 we will introduce the E-CMIRC process maturity assessment criteria.

## G5 E-CMIRC process maturity assessment criteria

We want to combine the processes and technologies of different services to realise cost and skills saving. We will thus focus our assessment criteria development efforts on the E-CMIRC processes and technologies. Furthermore, in Appendix A, the intention was expressed to view the E-CMIRC as a system and to develop it using systems engineering principles.

Systems engineering is primarily used to develop capabilities. This complements our decision to use the POSTEDFIT-B capability development model for our E-CMIRC CDM. The POSTEDFIT-B capability development model was derived from the South African DOD, and it is our experience that the South African DOD predominantly uses a systems engineering approach as a methodology when developing systems.

To avoid the use of different and incompatible models, and to compliment the E-CMIRC CDM, we select the SSE-CMM as the capability maturity model for the E-CMIRC. The fact that the SSE-CMM is also measurable against ISO/IEC 21827:2008 [305] further reinforces, and supports our decision. The maturity assessment criteria from the SEE-CMM will be used for the E-CMIRC processes.



These maturity assessment criteria will be mapped back to the COBIT numerical values, and these numeric values, together with the SEE-CMM maturity numeric level descriptions will be used for our E-CMIRC process assessments. The E-CMIRC maturity level values with the process maturity assessment criteria are shown in Table 53. The same table may also be used as a template when assessing the E-CMIRC process maturity.

**Table 53: E-CMIRC maturity levels and process maturity assessment template**

| COBIT Maturity Level Numeric Value | SSE-CMM Process Maturity Assessment Criteria |
|---|---|
| Level **0** | Not performed |
| Level **1** | Performed informally |
| Level **2** | Planned and tracked |
| Level **3** | Well defined |
| Level **4** | Quantitatively controlled |
| Level **5** | Continuously improving |

We will now provide a sample application of the E-CMIRC process maturity assessment template. We will illustrate the template's application by assessing the incident handling process.

**Table 54: E-CMIRC process maturity assessment criteria template application**

| Maturity Value | SSE-CMM Process Maturity Assessment Criteria |
|---|---|
| Level **0** | The incident handling process does not exist and is not performed. |
| Level **1** | The E-CMIRC incident handling process has a low maturity, and is performed informally. |
| Level **2** | The E-CMIRC incident handling process is planned and tracked. |
| Level **3** | The E-CMIRC incident handling process is well defined. |
| Level **4** | The E-CMIRC incident handling process is quantitatively controlled. |
| Level **5** | The E-CMIRC incident handling process has a high maturity is continuously improved. |

Now that we have identified the maturity score numeric value as well as the process maturity assessment criteria, we need to consider the technology maturity assessment criteria. The technology maturity assessment criteria are introduced in Section G6.

## G6 E-CMIRC technology maturity assessment criteria

The next step in completing the E-CMIRC CMM is to develop the assessment criteria against which its technologies will be assessed against. The assessment criteria will differ from between national requirements, and between technologies. The assessment criteria will be highlighted with a few examples to convey the intended usage, but to keep the model as flexible as possible; each developing country will develop its own measurement criteria. We will be using the familiar maturity scoring numeric values we selected for the process maturity assessment criteria. In Table 55 we propose a maturity assessment criteria template that countries may use during the development of the technology maturity assessment criteria.

The maturity assessment criteria column should be populated with criteria against which the maturity of the technology deployment will be assessed against. Each criterion will be scored using the maturity score we introduced in Section G5. We will illustrate the application of our template by using the event log collection capability. This is a technical capability and is delivered by the SIEM technology. The maturity level numeric value ranges from 0 to 5. The illustrative application is shown in Table 55.

**Table 55: E-CMIRC technology maturity assessment criteria template application**

| Maturity Value | Maturity assessment criteria: event log collection |
|---|---|
| 0 | No event log collection capability |
| 1 | A technology with a low capability will collect events from a limited number of vendors (<10) and device types (<5) using a limited number of protocols. |

| Maturity Value | Maturity assessment criteria: event log collection |
|---|---|
| 2 | A technology with a low capability will collect events from a low number of vendors (≤25) and device types (15) using a limited number of protocols. |
| 3 | A technology with a low capability will collect events from a limited number of vendors (≤75) and device types (20) using a limited number of protocols. |
| 4 | A technology with a low capability will collect events from a limited number of vendors (≤100) and device types (25) using a limited number of protocols. |
| 5 | A technology with a high capability will be able to collect events from multiple vendors (>150) with multiple device types (>25) using various protocols |

We have now illustrated the application of the process maturity assessment criteria template, and the technology maturity assessment criteria template. These two templates may be used during the maturity assessments of the E-CMIRC processes and technologies. We also need to consider the amount, or number of capability elements.

The E-CMIRC would not be valuable if it only consisted of the incident handling process capability, and the event log collection technical capability. It is thus important to consider the number of capabilities that the E-CMIRC would offer as well, and include the number of capabilities in the maturity score calculation. So far, we have the following elements that we will consider during the maturity assessment:

- The number of capabilities (people, processes and technology) offered by the E-CMIRC.
- The maturity assessment criteria of each capability element. Capabilities can have more than one maturity
- assessment criteria associated with it.
- The maturity level numeric value. This gives us the assessment score per maturity assessment criteria.

In Section G7 we present our E-CMIRC CMM.

## G7 E-CMIRC CMM presentation

In alignment with the decision made in Section 0, the E-CMIRC CMM is also presented as a symbolic model in a three-dimensional shape. This approach ensures familiarity of use and the application of the models, reducing training costs, and ensuring rapid deployment of the E-CMIRC CMM. The E-CMIRC CMM is presented in Figure 45.

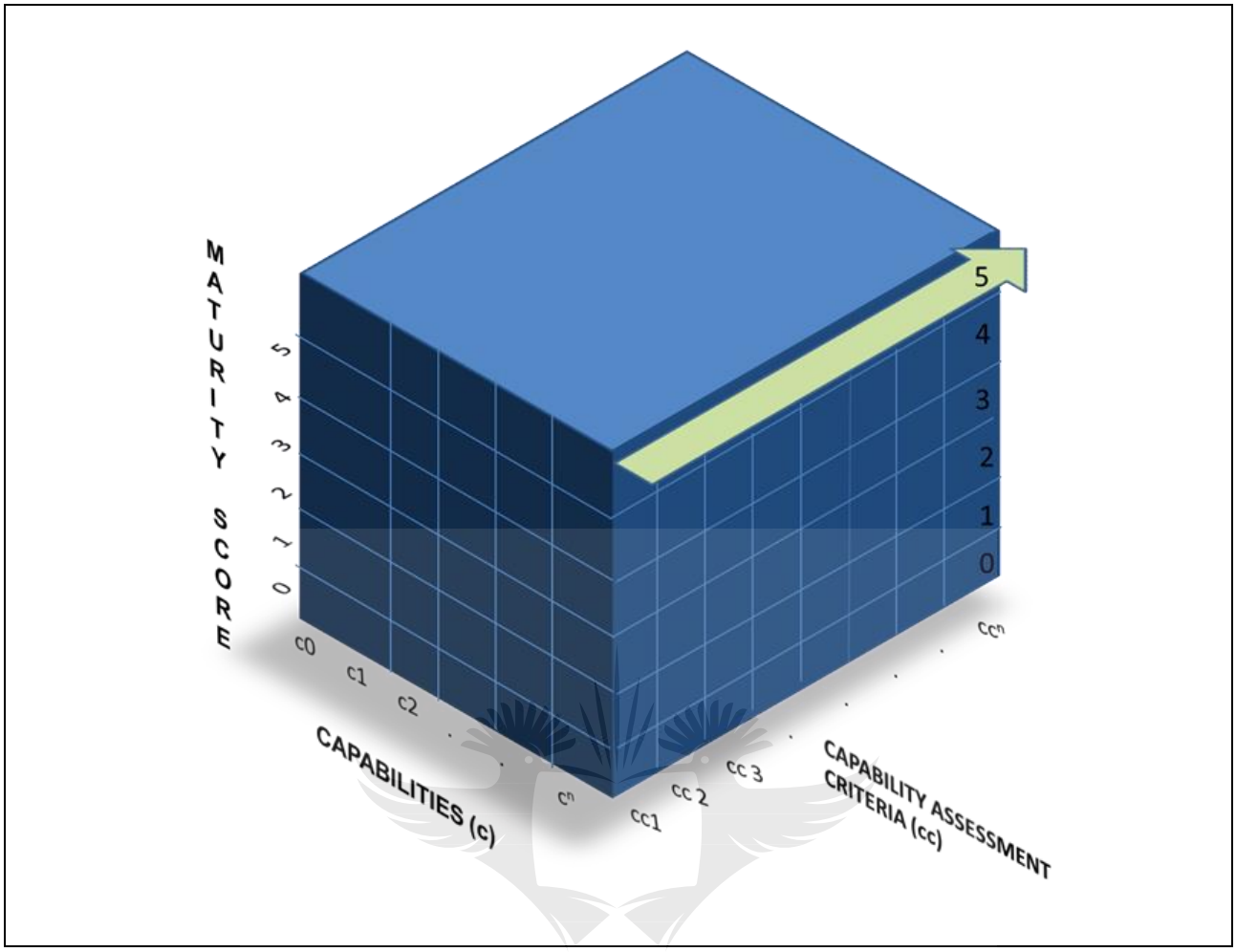



**Figure 45: E-CMIRC CMM**

The cube displays three sides. The first side displays the maturity score, starting with Levels 0 to 5. The maturity scores were introduced in Table 52. The bottom of the cube is reserved for the capabilities. The capabilities are presented with the symbol "*c.*" The right side of the cube is reserved for the capability assessment criteria. This is represented by *"cc."* We will now provide a description on how to use the E-CMIRC CMM through an analysis of the South African Cybersecurity Hub's incident handling process.The Cybersecurity Hub serves as the South African National CSIRT, and is used as a sample. The assessment is done based on our experience working in the Cybersecurity Hub. The same assessment process will be followed for a newly built or existing structure. The process is as follows:

- Identify the capabilities to be measured (the capability we have selected is the Cybersecurity Hub incident handling process).
- Analyse and categorise the process in a maturity level according to SSE-CMM process. Evidence supporting the categorisation should be provided.
- Define maturity assessment criteria, and assign a score.

**Table 56: E-CMIRC CMM: incident handling service**

| Maturity score | Capability assessment criteria |
|---|---|
| Process maturity score 0<br>Not performed | |
| Process maturity score 1<br>Performed informally | The Cybersecurity Hub's *incident handling* process is performed informally. As proof, e-mails pertaining to incidents are attached as well as reports from the *incident handling* application |
| Process maturity score 2<br>Planned and tracked | |
| Process maturity score 3<br>Well defined | |
| Process maturity score 4<br>Quantitatively controlled | |
| Process maturity score 5<br>Continuously improving | |

The incident handling process is performed informally, and is thus on maturity level 1. One of the capability assessment criteria for the incident handling process was used as an example. The maturity assessment criteria for the incident handling process is scored from "0" to "5." One capability may have multiple maturity assessment criteria against which it can be measured..

In this regard, NIST SP 800-61 [72] lists the incident handling tasks as preparation, detection and analysis, containment, eradication and recovery, as well as post incident activity. These can all serve as maturity assessment criteria. The number of maturity assessment criteria are determined by the entity building the E-CMIRC, as well as the nation's requirements in terms of functions and service capabilities. A sample of a high-level incident handling capability's maturity assessment criteria is shown in Table 57. We are using the following as maturity assessment criteria:

- **Capability assessment criteria 1:** The incident handling process is automated.
- **Capability assessment criteria 2:** The incident handling process is supported by technology.
- **Capability assessment criteria 3:** The number of reported incidents resolved (<15%, <20%; >20%, <50% >50%, >75%).
- **Capability assessment criteria 4:** National actors are involved.
- **Capability assessment criteria 5:** International actors are involved.

As stated, our aim is not to develop a comprehensive list of capability maturity assessment criteria. Our aim is rather to illustrate how to apply the E-CMIRC CMM.

**Table 57*:* Incident handling capability measurement**

| Score | Incident Handling process maturity assessment criteria |
|---|---|
| **0** | No incident handling process exists. |
| **1** | Incidents are created manually.<br>Incidents are reacted to manually.<br>Fewer than 15% of reported incidents are resolved. |
| **2** | Incidents are created manually.<br>Technology and support tools are used to investigate the incident.<br>Less than 20% of reported incidents are resolved. |
| **3** | Incidents are created automatically.<br>Technology and support tools are used to investigate the incident.<br>More than 20% of reported incidents are resolved. |
| **4** | Incidents are created automatically.<br>Technology and support tools are used to investigate the incident.<br>National stakeholders are involved.<br>More than 50% of reported incidents are resolved. |
| **5** | Incidents are created automatically.<br>Technology and support tools are used to investigate the incident.<br>National and international stakeholders are involved.<br>More than 75% of reported incidents are resolved. |

We will now consider the Cybersecurity Hub's "incident handling process" as a maturity assessment criteria. We have awarded the Cybersecurity Hub's "incident handling process" a score of "1". This is because our experience has shown that incidents are manually created by using a web portal, or via e-mails. These reported incidents are then manually captured in the incident handling application. Less than 20% of all reported incidents are resolved by the Cybersecurity Hub.

We also found that the Cybersecurity Hub (at the time of writing)) offers two national capabilities. These are the incident handling capability, and the awareness and training capability. These findings are presented in Figure 46 using the E-CMIRC CMM.

Figure 46 shows that the Cybersecurity Hub offers two national cybersecurity capabilities. We have assessed the Cybersecurity Hub's incident handling process. We have scored the Cybersecurity Hub incident handling process a score of "1" based on our experience at the time of writing.

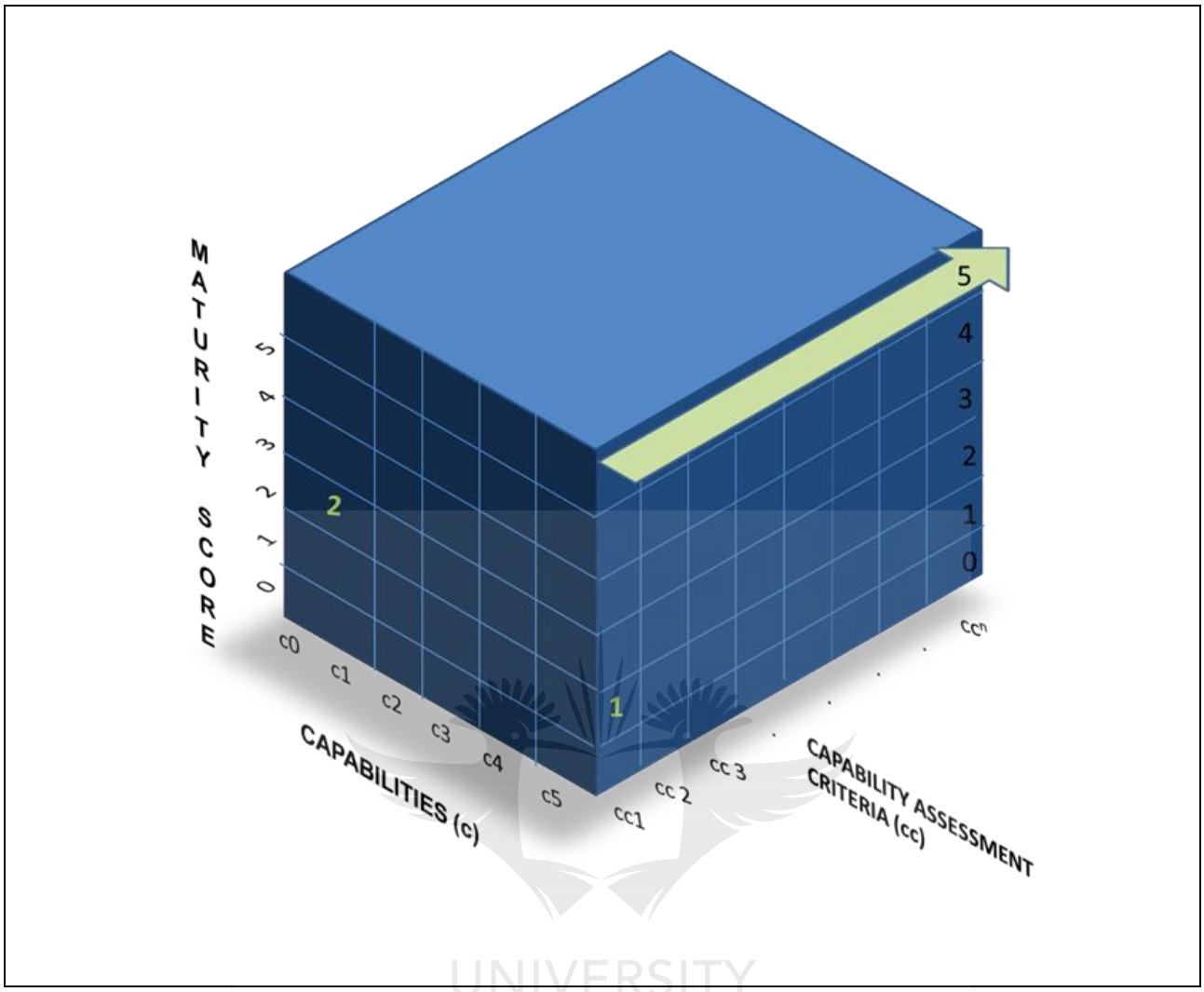



**Figure 46: Cybersecurity Hub analysis against E-CMIRC CMM**



The E-CMIRC CMM can also be expressed mathematically. This will allow us to assign a weighting to our E-CMIRC's capability and its maturity. We will assign a higher weighting for maturity since we view the maturity (describing the executability and repeatability of a capability) as more important than the number of capabilities and its capability assessment criteria [167]. The mathematical expression as taken from [167], is shown:

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

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

$$\alpha = 0.4$$
$$\beta = 0.6$$

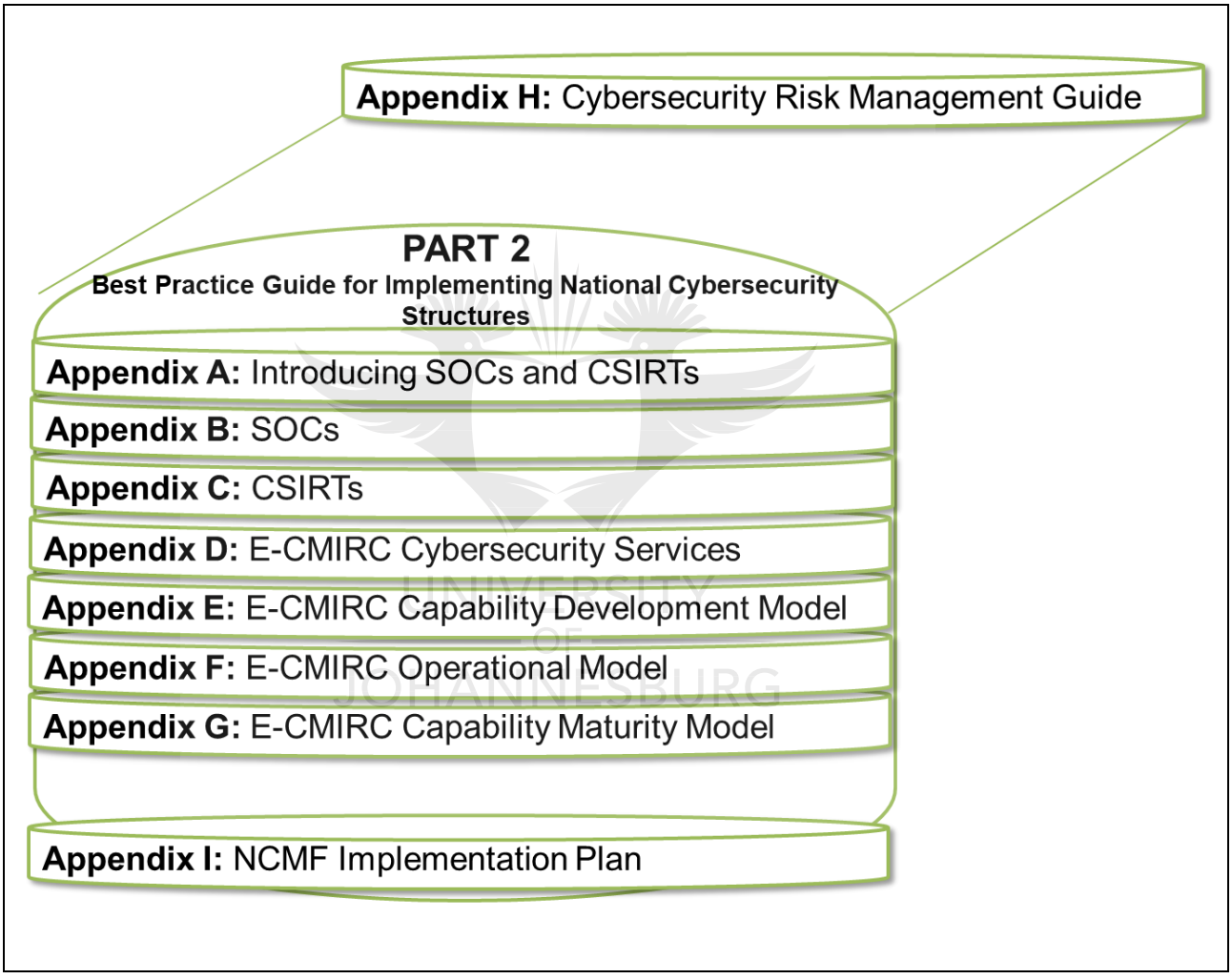
To balance the scoring, and to indicate the higher importance of maturity over the total number of capabilities, a α value of 0.4 is selected for the maturity of the capability. This would give the total number of capability assessment criteria score a lesser impact than the maturity score. The E-CMIRC score is thus equal to the sum of all capabilities and where each capability is scored on its capability assessment criteria. The formula will provide a maturity score out of 100.

- Capability maturity score is represented by $C_i$.
- Capability weighting is presented by α..
- Capability assessment criteria total is represented by $CC_i$.
  Capability assessment criteria total weighting is presented by β.
- Maturity score is presented by $n$.

This formula provides a score out of 100. The E-CMIRC CMM may be used to provide a maturity score for all people, processes, technology and structures capability elements. We have used the incident handling process capability to illustrate the application of the E-CMIRC CMM.

## G8 Conclusion

In this appendix, the E-CMIRC CMM was developed and presented. Its application was illustrated by measuring the incident handling process capability maturity of an existing structure – the Cybersecurity Hub. We did this based on our experience working experience working with the Cybersecurity Hub. A mathematical model was also proposed that allows the E-CMIRC capabilities to be represented mathematically. The E-CMIRC CMM offers a mechanism through which the effectiveness and efficiency of the E-CMIRC capabilities can be measured, baselined and improved on.


Appendix H: Cybersecurity Risk Management Guide
PART 2
Best Practice Guide for Implementing National Cybersecurity Structures
Appendix A: Introducing SOCs and CSIRTs
Appendix B: SOCs
Appendix C: CSIRTs
Appendix D: E-CMIRC Cybersecurity Services
Appendix E: E-CMIRC Capability Development Model
Appendix F: E-CMIRC Operational Model
Appendix G: E-CMIRC Capability Maturity Model
Appendix I: NCMF Implementation Plan

# Appendix H: Cybersecurity Risk Management Guide

## H1 Introduction

It is our experience that the *national strategic risk and threat assessment* function is typically composed of a risk management strategy, that in turn describes a national risk management approach, which may include the development of a national risk management framework. This framework then describes the national cybersecurity risk management process. Our research did not produce a national cybersecurity risk management framework and process that can be used as a guide.

Considering the importance of the National Strategic Risk and Threat Assessment function during the selection and prioritisation tasks, we, therefore, propose a national risk management guide and by combining two existing standards. Our proposed guide is not mandatory, but is helpful as guidance where developing countries do not have a national cybersecurity risk management framework.

## H2 NCMF Level 2 – National Cybersecurity Risk Management Guide

The outcome of the risk management process described in the national risk management guide, will, together with the dimensions, domains and mandates, largely dictate the selection and prioritisation of cybersecurity functions for implementation. This section proposes a national risk management guide that may be used to conduct a national cybersecurity risk assessment, the result of which will inform the selection and prioritisation of cybersecurity functions. Based on our experience, the requirements for a cybersecurity risk management framework, with its processes to be used at national level, are as follows:



- The risk management process described in the framework should be generic enough for use at national level.
- The risk management process described in the framework must be high-level enough to be used nationally, but must be specific to information security.
- The risk management process described in the framework should be flexible enough to complement and enhance existing government information security risk management initiatives.
- The risk management process described in the framework should be carried out in accordance with the nation's chosen information security standards and frameworks.

## H3 Comparing risk management standards and frameworks

We have decided to make use of existing, internationally accepted risk management standards, and from these, identify the ones most ideal, and propose a framework using the processes described in them. In deciding on a risk management framework to apply at national level, the following exiting ISO/IEC and ITU risk

management standards were considered and evaluated. The risk management standards we have identified and evaluated are presented in Table 58.

**Table 58: Standards considered for a National Risk Management Framework**

| Standard | Description |
|---|---|
| **ITU-T X.1055** - Risk management and risk profile guidelines for telecommunication organisations [306] | The ITU-T X.1055 Recommendation describes the processes, techniques and functional profiles for information security risk management for telecommunication in support of the ITU-T X.1051 \| ISO 27011 Recommendation and other ITU-T recommendations. |
| **ISO/IEC 27011:2008** - Information security management guidelines for telecommunications organisations [307]. | This standard specifies Information security management guidelines for telecommunications organisations based on ISO/IEC 27002. |
| **ISO/IEC 27005:2011** Information security risk management [308] | ISO 27005:2011 provides guidelines for information security risk management. It supports the general concepts specified in ISO 27001 and is designed to assist the satisfactory implementation of information security based on a risk management approach. ISO 27005:2011 focuses on information security risk, and does not address organisational risk. |
| **ISO/IEC 31000:2009** Risk management -- Principles and guidelines [10] | ISO 31000:2009 provides principles and generic guidelines on risk management, and can be used by any public, private or community enterprise, association, group or individual. ISO 31000:2009 is thus not specific to any industry or sector. |
| National Institute of Standards and Technology **(NIST)** Special Publication **(SP) 800-39**. Managing Information Security Risk [9] | NIST SP 800-39 address information security risk, but also focuses on organisational risk. |

Considering the requirements for a national risk management framework, and after an analysis of the strengths and weaknesses of the identified standards was performed, the following standards were excluded:

- ITU-T X.1055 [306] provides guidelines specific to telecommunications organisations and, therefore, does not comply with the requirement of being generic.
- ISO/IEC 27011:2008 [307] provides guidelines to telecommunications organisations, and also does not comply with the requirement of being generic.
- ISO/IEC 31000:2009 [10] is applicable to any industry risk and thus does not comply with the requirement that the risk management process should be information security specific.

This left us with NIST SP 800-39 [9] and ISO/IEC 27005:2011 [308] as the only standards that therefore met all the requirements. A strong argument may however be made for the selection of ISO/IEC 31000:2009 [10], since, a comparison between ISO/IEC 27005:2011 with ISO/IEC 31000:2009, shows more similarities than differences. Another argument for the use of ISO/IEC 27005:2011 together with ISO/IEC 31000:2009 is that these standards are from the same family, and follow a common approach, methodology and terminology. Therefore, a strong argument needs to be made for using standards from two different families, such as ISO/IEC and NIST.

ISO/IEC 31000:2009 [10] addresses general risk management, covering concepts, definitions and a methodology for a risk management process to be applied to any industry or activity. It is broad enough to be used by any activity touching the management of risks (in areas and industries such as compliance, oil and gas, corporate risks, projects, safety, etc.) and covers all risks to the organisation. It does not focus on IT risk management. ISO/IEC 27005:2011 [308] addresses IT risk management. It uses the same framework described in ISO/IEC 31000:2009 [10] and applies it to IT needs [309].

Whereas ISO/IEC 31000:2009 [10] follows a generic risk management approach, ISO/IEC 27005:2011 [308] describes a distinct process for managing information security risk based on a partial application of the principles introduced in ISO/IEC 31000:2009 [310]. A further differentiator when contrasting ISO/IEC 31000:2009 and ISO/IEC 27005:2011 is that ISO/IEC 27005:2011 addresses vulnerabilities.

National cybersecurity vulnerabilities and threat management will be key when considering national cybersecurity functions for implementation. Another difference to consider when having to make a selection; is that ISO/IEC 31000:2009 follows a high-level approach and ISO/IEC 27005:2011 following a detailed approach [310]. The differences as discussed between ISO/IEC 27005:2011 [308] and ISO/IEC 31000:2009 [10] are summarised in Table 59.

**Table 59: Comparison between ISO/IEC 31000:2009 and ISO/IEC 27005:2011**

| ISO/IEC 31000:2009 | ISO/IEC 27005:2011 |
|---|---|
| Generic risk management process | Risk management process specific to information security |
| Broad approach | IS domain specific process |
| Does not specifically address IS vulnerabilities | Address general IS vulnerabilities |
| High-level (generic and fast) | Detailed (long run and resource requiring) |

Considering the above,argument it is clear that ISO/IEC 27005:2011 [308] is the most befitting standard when considering its purpose and application in the development of a national cybersecurity risk management process. A benefit of employing ISO/IEC 27005:2011 is that it allows system administrators and managers to use a common approach and language and come to an agreement on risk.

None of the above standards and recommendations however addresses organisational risk at national level. NIST SP 800-39 [9] was identified as an appropriate publication addressing organisational risk at national level. The characteristic of it being able to address cybersecurity risk at national level, makes NIST SP 800-39 a candidate framework to consider during the development of our national cybersecurity risk management framework.

Organisational risk includes many different types of risks, such as programme management risk, investment risk, budgetary risk security risk, supply chain risk and legal liability risk to name a few. Risk to the utilisation and operation of information systems can be broken down into different types, of which information security risk is one.

SO/IEC 27005:2011 covers risk from an information security perspective, but does not cover organisational risk. NIST SP 800-39 correlates with ISO/IEC 27005:2011, but covers organisational risk, mission and business risk, and information systems risk. To this effect, ISO/IEC 27005:2011 is proposed to, describe the risk management process pertaining to cyber security in detail,, and NIST SP 800-39 used to describe the risk management process related to cybersecurity risk at the organisational level. The risk management process will thus be developed using a tailored merger between ISO/IEC 27005:2011 and NIST SP 800-39.

## H4 Combining ISO/IEC 27005:2011 and NIST SP 800-39

We proposed to make use of a combination of ISO/IEC 27005:2011, and NIST SP 800-39 [9] to formulate a risk management framework which can be used, at, and scale to national level. We will now introduce the ISO/IEC 27005:2011, and NIST SP 800-39 risk management processes.



ISO/IEC 27005:2011 describes four processes. These are context establishment, risk assessment, risk treatment and risk monitoring and review [8]. The NIST SP 800-39 also describes four processes. These are risk framing, assessing risk, risk response and risk monitoring. The overlap between the risk management processes are shown in Table 60:

**Table 60: Process comparison between ISO/IEC 27005:2011 and NIST SP 800-39**

| NIST SP 800-39 | ISO/IEC 27005:2011 |
|---|---|
| Risk framing | Context establishment |
| Assessing risk | Risk assessment |
| Risk response | Risk treatment |
| Risk monitoring | Risk monitoring and review |

Table 60 shows that there is an overlap between the NIST SP 800-39 and ISO/IEC 27005:2011 processes. The major difference is between the scope of the NIST SP 800-39 Risk Framing process and the scope of the

complementary ISO/IEC 27005:2011 context establishment process. ISO/IEC 27005:2011 establishes the context at the information systems level, while NIST SP 800-39 frames risk at all three process layers (listed in Table 60), allowing for a much wider scope. This also enables it to scale to the national level.

In tailoring the two standards, we have replaced the ISO/IEC 27005:2011 context establishment process with the NIST SP 800-39 risk framing process. During the risk framing process, the scope and boundaries will be defined, and the organs of state managing information security risk is established. This approach is shown in Figure 47. Figure 47 shows ISO/IEC 27005:2011 risk management processes as taken from [308], as well as the NIST SP 800-39 risk management processes as taken from [9]. These processes were introduced in Table 60. Figure 47 shows that we have replaced the ISO/IEC 27005:2011 context establishment process with the NIST SP 800-39 risk framing process.

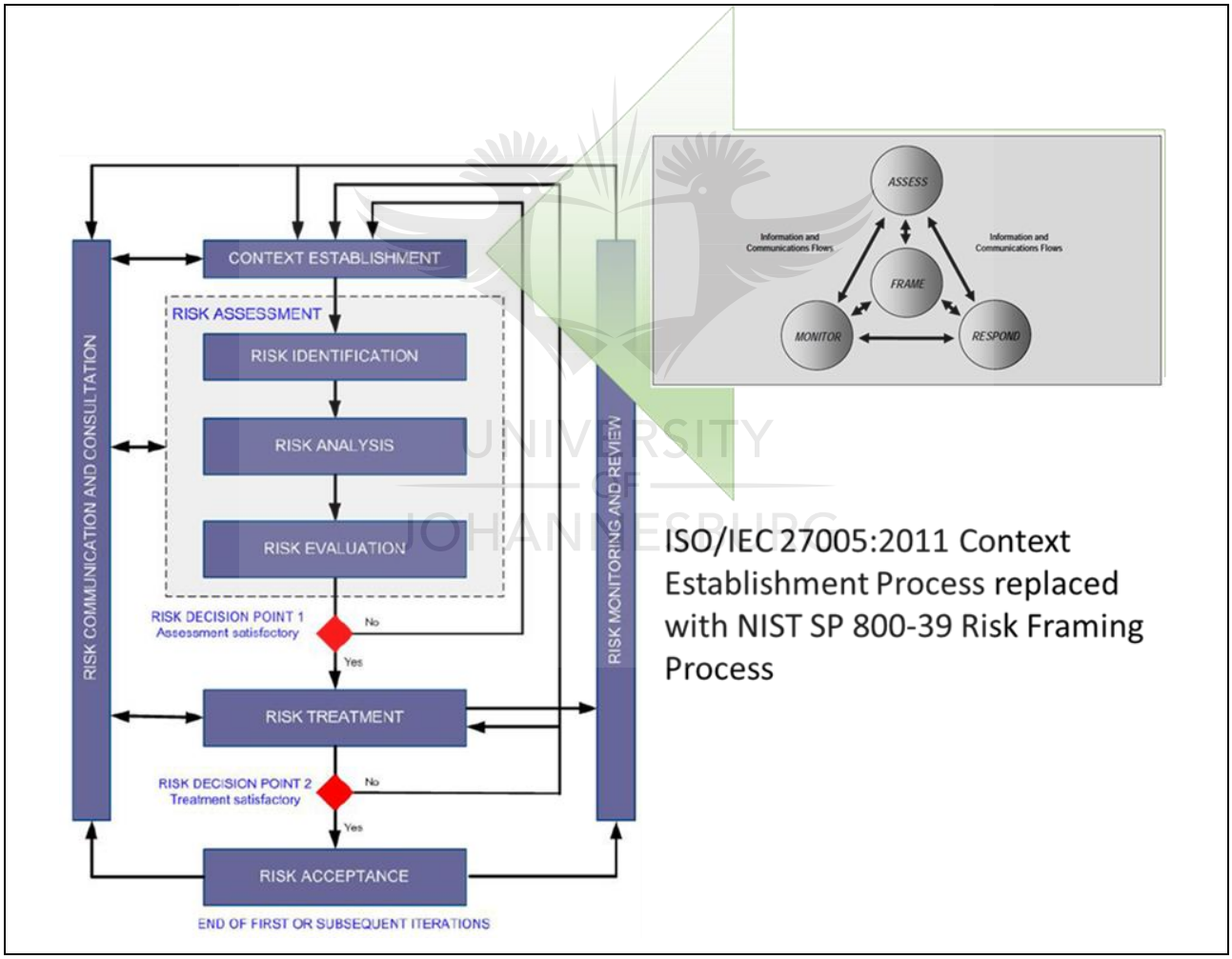



**Figure 47: Application of NIST SP 800-39 and ISO 27005** [9]

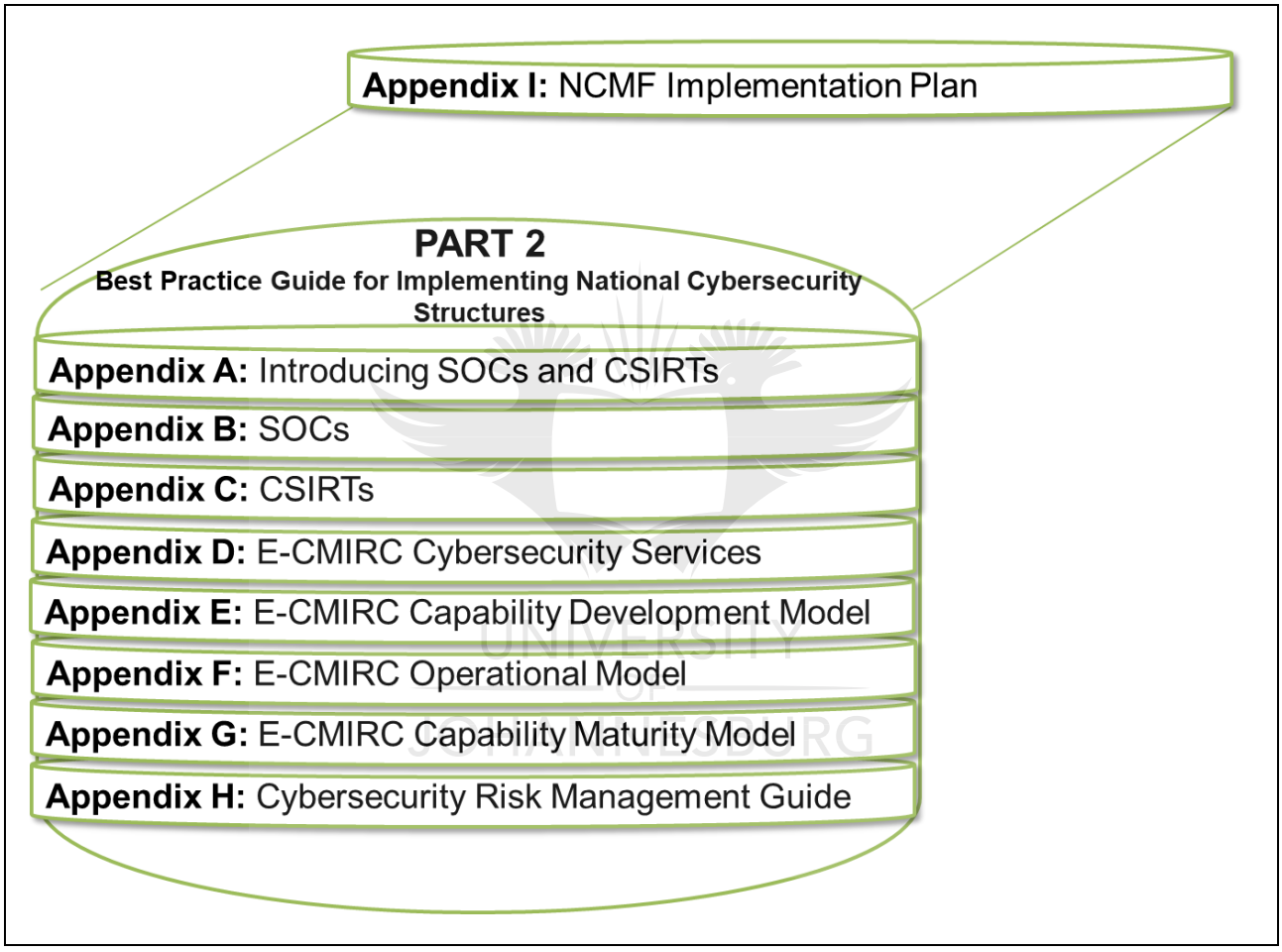
This risk framing process will be tailored with the national view, addressing strategic risk at national level. This is done to accommodate the requirement for the risk management process to be generic enough to be used

at national level. NIST SP 800-39 addresses organisational risk at national level. ISO/IEC 27005:2011 being information security specific, is used to determine the national cybersecurity risk.

Table 61 presents our National Cybersecurity Risk Management Framework. It shows that the ISO/IEC 27005 context establishment process is replaced with the NIST SP 800-39 risk framing process. The process details are described in the individual standards, and may be used as reference by states wishing to implement our National Cybersecurity Risk Management Framework.

**Table 61: National cybersecurity risk management framework**

| National Cybersecurity Risk Management Guide |
|---|
| Risk framing process described by NIST SP 800-39 to cover organisational risk at national level |
| Risk assessment described by ISO/IEC 27005:2011 |
| Risk treatment described by ISO/IEC 27005:2011 |
| Risk monitoring and review described by ISO/IEC 27005:2011 |


Appendix I: NCMF Implementation Plan
PART 2
Best Practice Guide for Implementing National Cybersecurity Structures
Appendix A: Introducing SOCs and CSIRTs
Appendix B: SOCs
Appendix C: CSIRTs
Appendix D: E-CMIRC Cybersecurity Services
Appendix E: E-CMIRC Capability Development Model
Appendix F: E-CMIRC Operational Model
Appendix G: E-CMIRC Capability Maturity Model
Appendix H: Cybersecurity Risk Management Guide

## Appendix I: NCMF implementation plan for South Africa

It is our experience that the South African government operates at four different strategic levels of control. These levels are political, strategic, tactical and operational [1] [311]. At these different levels of government, there are different expectations, requirements and outcomes [1]. The Merriam-Webster dictionary defines a strategy as "the art of devising or employing plans or stratagems toward a goal" while the Oxford dictionary defines it as "The art of planning and directing…" The purpose of the NCMF is to plan and direct the national cybersecurity function management effort. Figure 48 presents the NCMF Implementation Plan.

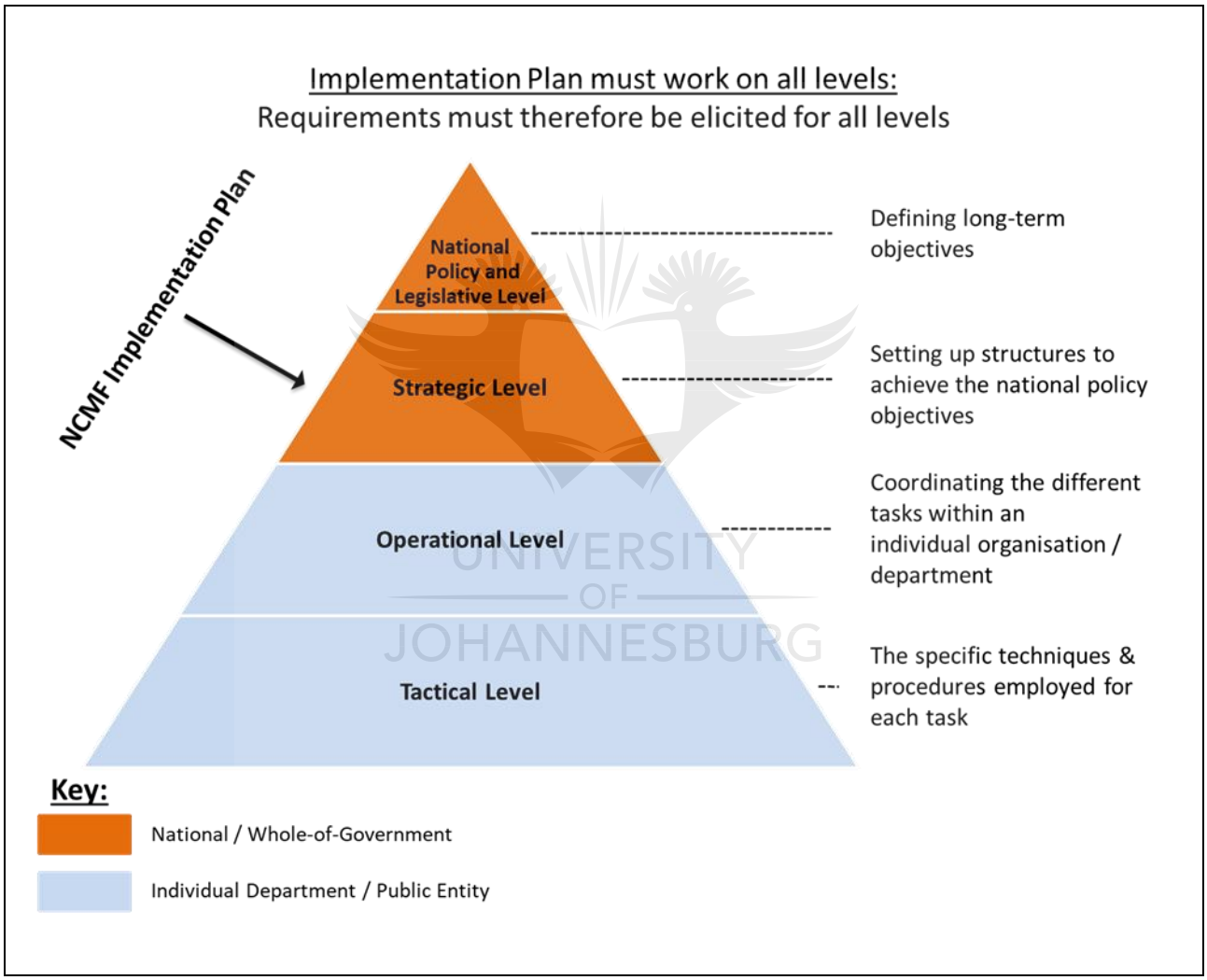



**Figure 48: NCMF Implementation Framework** [42]

Figure 48 shows that the NCMF Implementation Plan should be applied at the strategic level. At the national policy and legislative level, national strategy and long-term objectives are defined. This is the responsibility of the government that should be held accountable for the establishment of a national strategy, and long-term objectives, and structures to give effect to the national policy.

The NCMF should be included as part of the national policy and legislative effort, but be executed at the strategic level. Responsibility may be delegated, but accountability not [312], [313]. The responsibility for the establishment of a national strategy, and long-term objectives as well as the establishment of national structures may thus be delegated, by the government, to the overall controlling body that we have established at level 2 of the NCMF.

The overall controlling body may then delegate the responsibility and accountability for the actual implementation of the national cybersecurity structures to government departments. In the context of South Africa, the South African government is accountable to the nation in terms of developing a national cybersecurity policy and strategy, but the responsibility is delegated to the CRC and NCAC. They, in turn, may delegate responsibility for the establishment of national cybersecurity structures to government departments such as the DTPS, SSA, DOD and SAPS.

,

## I2 Separation of NCMF and cybersecurity functions

Now that the NCMF Implementation Plan has been introduced, and before we start a discussion on the *incident handling*, and *monitoring and evaluation* of National ICT function's structures, it is important to understand that there should be a clear distinction between the implementation of the NCMF as a framework, and the implementation of the cybersecurity functions identified by the NCMF. This distinction and separation must be made since the actors and resources needed to effect the implementation of the NCMF and the cybersecurity functions are different.



Accordingly, the actors needed for the implementation of the NCMF could be state and government actors in the government dimension, since this is from where the political will, resources and funding would come. Actors interacting with the national cybersecurity function implementation, as well as its resources may come from state and government actors and organised non-state actors in the international dimension. This separation and distinction is needed to allow for the correct actors and resources to be identified and assigned responsibility for the implementation of the NCMF.

## I3 NCMF implementation critical success factors

The following are critical success factors to ensure a successful implementation of the NCMF. We assume that a nation-state considering the application of the NCMF already has the political will and the financial means, skills, capability and capacity to do so. It is our experience that political will and national implementation capability are key success factors where it concerns the implementation of frameworks and strategies at national level. Before starting with the implementation of the framework, the following critical success factors should be considered:

- A common national cybersecurity terminology and language should be established. This can foster a common understanding of expectations and expected outcomes.
- The national terminology and language should be aligned with the terminology and language used by international peers.
- A strategy should be devised for the implementation of the NCMF. Identify all stakeholders and actors. As an alternative, our NCMF Implementation Plan may be considered.
- Responsibilities should be assigned to stakeholders and actors.
- Resources should be identified and assigned for the implementation of the NCMF.
- Existing national cybersecurity risk management frameworks, strategies and processes should be Identified if our proposed framework is not used.

The actual implementation of the framework is a sequential process, progressing from one level to the next. The outcome of the completed level serves as input into the level following it. This means that the NCMF must be implemented sequentially, and budget and resource allocation needs to be done for each level.