A model for security incident response in the South African National Research and Education Network

by

Roderick D. Mooi

A model for security incident response in the South African National Research and Education Network

by

Roderick D. Mooi

Dissertation

submitted in fulfillment
of the requirements
for the degree

Master of Technology

in

Information Technology

in the

Faculty of Engineering, the Built Environment and Information Technology

of the

Nelson Mandela Metropolitan University

Promoter: Prof. Reinhardt A. Botha

December 2014

DECLARATION

I, Roderick David Mooi (212468960), hereby declare that this dissertation for Master of Technology (Information Technology) is my own work and that it has not been submitted for assessment or completion of any postgraduate qualification to another University or for another qualification.

. . . .

Roderick D. Mooi

ACKNOWLEDGEMENTS

My sincere thanks goes to:

- Father God — my Creator, Redeemer, Friend, Guide and Strength.
- My wife, Joanney, for her loyal support, understanding and motivation to keep going (with coffee when necessary) and doing more than her share of baby-sitting!
- My supervisor, Prof. Reinhardt Botha, for his encouragement, support, approachability and council.
- The CSIR for making this research possible — providing financial support and time for me to work on it.
- My proof readers — mother and wife — for your useful feedback and corrections.
- My friends, family and colleagues for your support, interest and ideas.

I appreciate you all!

ABSTRACT

This dissertation addresses the problem of a lack of a formal incident response capability in the South African National Research and Education Network (SA NREN). While investigating alternatives it was found that no clear method exists to solve this problem. Therefore, a second problem is identified: the lack of a definitive method for establishing a Computer Security Incident Response Team (CSIRT) or Computer Emergency Response Team (CERT®) in general. Solving the second problem is important as we then have a means of knowing how to start when building a CSIRT. This will set the basis for addressing the initial problem, resulting in a prepared, improved and coordinated response to IT security incidents affecting the SA NREN.

To commence, the requirements for establishing a CSIRT are identified via a comprehensive literature review. These requirements are categorised into five areas, namely, the basic business requirements followed by the four Ps of the IT Infrastructure Library (ITIL®). That is, People, Processes, Product and Partners, adapted to suit the CSIRT context. Through the use of argumentation, the relationships between the areas are uncovered and explored. Thereafter, a Design Science Research-based process is utilised to develop a generic model for establishing a CSIRT.

The model is based on the interactions uncovered between the business requirements and the adapted four Ps. These are summarised through two views — *strategic* and *tactical* — together forming an holistic model for establishing a CSIRT. The model highlights the decisions required for the business requirements, services, team model and staff, policies and processes, tools and technologies, and partners of a CSIRT respectively.

Finally, to address the primary objective, the generic model is applied to the SA NREN environment. Thus, the second artefact is an instantiation, a specific model, which can be implemented to create a CSIRT for the SA NREN. To produce the specific model, insight into the nature of the SA NREN environment was required. The status quo was revealed through the use of a survey and argumentative analysis of the results. The specific decisions in each area required to establish an SA NREN CSIRT are explored throughout the development of the model. The result is a comprehensive framework for implementing a CSIRT in the SA NREN, detailing the decisions required in each of the areas. This model additionally acts as a demonstration of the utility of the generic model.

The implications of this research are twofold. Firstly, the generic model is useful as a basis for anyone wanting to establish a CSIRT. It helps to ensure that all factors are considered and that no important decisions are neglected, thereby enabling an holistic view. Secondly, the specific model for the SA NREN CSIRT serves as a foundation for implementing the CSIRT going forward. It accelerates the process by addressing the important considerations and highlighting the concerns that must be addressed while establishing the CSIRT.

Contents

List of Tables

List of Figures

Acronyms and abbreviations

AUP	Acceptable Use Policy
AIRT	Application for Incident Response Teams
AS	Autonomous System
Bash	Bourne-Again SHell
CA	Competency Area
CCIW	Command, Control and Information Warfare
CERT®	Computer Emergency Response Team
CHIHT	Clearing House for Incident Handling Tools
CII	Critical Information Infrastructure
CIIP	Critical Information Infrastructure Protection
CIP	Critical Infrastructure Protection
CMU	Carnegie Mellon University
C-SAW	Community-orientated Security, Advisory and Warning
CSIR	Council for Scientific and Industrial Research
CSIRT	Computer Security Incident Response Team
DDoS	Distributed Denial of Service
DHET	Department of Higher Education and Training
DoC	Department of Communications
DoS	Denial of Service
DRDoS	Distributed Reflective Denial of Service
DS	Design Science
DSR	Design Science Research
DST	Department of Science and Technology
ECT	Electronic Communications and Transactions
EHS	Environment, Health and Safety
ENISA	European Network and Information Security Agency
FIRST	Forum for Incident Response and Security Teams
FOSS	Free and Open Source Software

GnuPG	GNU Privacy Guard
HR	Human Resources
HTTP	HyperText Transfer Protocol
HTTPS	HTTP Secure
IDS	Intrusion Detection System
IRT	Incident Response Team
IS	Information Systems
ISO	International Organization for Standardization
ISP	Information Security Policy
ISP	Internet Service Provider
ITIL®	IT Infrastructure Library
LHC	Large Hadron Collider
MDS	Modelling and Digital Science
MSSP	Managed Security Service Provider
NOC	Network Operations Centre
NREN	National Research and Education Network
OTRS	Open Technology Real Services
PGP	Pretty Good Privacy
POPI	Protection of Personal Information
PSIRT	Product Security Incident Response Team
RFC	Request for Comments
RICA	Regulation of Interception of Communications and provision of communication-related information Act
RIPE	Réseaux IP Européens
RT	Request Tracker
RTIR	Request Tracker for Incident Response
SA NREN	South African NREN
SANReN	South African National Research Network
SANS	South African National Standards
SANS	SysAdmin, Audit, Networking and Security
SEI	Software Engineering Institute
SERT	Security Emergency Response Team
SITA	State Information Technology Agency
SKA	Square Kilometre Array
SSL	Secure Sockets Layer
TENET	Tertiary Education and Research Network of South Africa
TERENA	Trans-European Research and Education Networking Association

TI	Trusted Introducer
TLS	Transport Layer Security
TVET	Technical Vocational Education and Training
WARP	Warning, Advice and Reporting Point
WITS	University of the Witwatersrand

Part I

Prologue

Chapter 1

Introduction

From the early days of the Internet, malicious activity emerged as a growing threat and reality. What originated as practical jokes between early experimenters soon became dangerous tools in the hands of those seeking to use this new network of interconnected machines for their own devious purposes. Since then, the race between white-hat security experts and black-hat hackers has continued with the good guys always pressured to stay one step ahead of the bad guys. As vulnerabilities are exposed/discovered in protocols, networking devices and applications, advisories and recommendations hit the IT security news headlines until a patch can be released and distributed. Then a moment's peace until the next incident occurs. The war is on and it's very much alive — more so today than ever before. The risks and rewards to be reaped through compromised systems increase with every move closer to a *cyber*-society.

National Research and Education Networks (NRENs) are not immune to malicious activity. In fact, due to the high bandwidth links and international connectivity typically provided to science and academic customers, NRENs can be very attractive targets. The impact of an incident in such an environment can be devastating.

Computer Security Incident Response Teams (CSIRTs), as the primary approach used to deal with IT security incidents, are introduced next. A description of NRENs follows, focusing on the South African NREN environment. This sets the scene for the problem statement and subsequent research objectives. Finally, a chapter layout dictates the structure of the dissertation.

1.1 Dealing with IT security incidents

Popular IT news sites (Reuters, 2012; Kumparak, 2014), security-related conferences (ISSA, 2012; FIRST, 2012) and talks of global cyber-war (News24, 2012; Ranger, 2014; ENISA, 2014) evidence the reality of the IT security landscape today. 2014 marked a year of particular significance with Distributed Reflective Denial of Service (DRDoS) attacks on the rise[1] followed by the revealing of critical vulnerabilities in core libraries of systems connected to the Internet. Names like "Heartbleed" (OpenSSL vulnerability), "Shellshock" (Bash vulnerability), and the exploitation of these vulnerabilities,[2,3] show just how fragile this ecosystem really is.

1.1.1 What is an IT security incident?

Hacking, virus outbreaks and denial of service attacks are primary examples of computer or *information security incidents*. Formally, an IT security incident is defined as a *"single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security"* (SANS, 2009, p. 3).

How do we recognise and deal with these incidents? Firstly, with policies and procedures that define "normal" operations, followed with a mechanism to act on infringement of these policies. Therefore, the establishment of a team responsible for incident handling is the preferred approach to establishing an *incident response capability* (Killcrece, Kossakowski, Ruefle, & Zajicek, 2003a, p. 1).

1.1.2 Computer Security Incident Response Teams

The definition of a *Computer Security Incident Response Team (CSIRT)* used by Alberts, Dorofee, Killcrece, Ruefle, and Zajicek (2004) is embraced in this dissertation.

[1] `https://www.us-cert.gov/ncas/alerts/TA14-017A`

[2] `http://www.fireeye.com/blog/technical/2014/09/shellshock-in-the-wild.html`

[3] `https://www.mandiant.com/blog/attackers-exploit-heartbleed-openssl-vulnerability-circumvent-multifactor-authentication-vpns/`

That is, a CSIRT is

> *"an organization or team that provides services and support to a defined constituency for preventing, handling, and responding to computer security incidents"* (Alberts et al., 2004, p. 1).

Establishing a security incident response capability as a means to handle computer and network security-related incidents is no small feat. More information on CSIRTs is provided in Chapter 3.

Next, as the scope of this study, the South African National Research and Education Network (SA NREN) environment is considered.

1.2 National Research and Education Networks

A National Research and Education Network (NREN) provides backbone network infrastructure, access connectivity and specialised services to the academic and research institutions of a country. This includes high-bandwidth links for science and research, commodity Internet connectivity, network support and maintenance, and related services. An NREN is *"a specialised Internet service provider to the research and educational communities within a country"* (TERENA, 2010, para. 8).

The South African National Research Network (SANReN) Competency Area (CA) together with the Tertiary Education and Research Network of South Africa (TENET) constitute the South African NREN. The SANReN project team designs and builds the network and the TENET team operate it. Both parties are involved in the development and provisioning of value-added services on top of the network (Petruccione et al., 2013, p. 26).

1.2.1 The South African National Research Network

The South African National Research Network (SANReN) is a project of the Council for Scientific and Industrial Research (CSIR) Meraka Institute, initiated by the Department of Science and Technology (DST). It is a high-speed network dedicated to research traffic and is intended to accelerate participation of South African researchers in the global knowledge production effort (SANReN, 2010). Beneficiary institutions aligned with the goals of SANReN are identified and connected to the network using a phased approach.

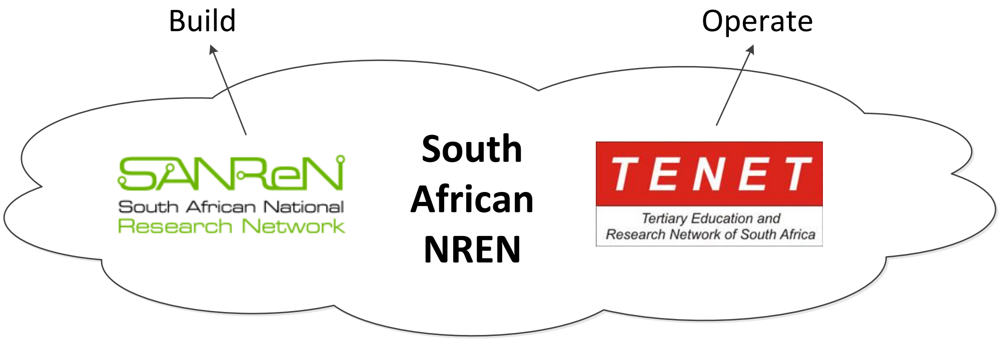


Figure 1.1: The South African National Research and Education Network (by author)

As of 31 March 2014, 173 higher education and research sites were connected to SANReN providing multi-gigabit Internet access and data transfer capabilities with typical site connections of 1 and 10 Gbps (Staphorst, 2014). The number of connected sites continues to grow, covering nearly one million users at public universities, science councils and national research facilities throughout South Africa. This amount of users makes the network vulnerable to malicious activity; particularly attacks on the data and infrastructure. Furthermore, there is substantial critical infrastructure at the connected sites, as well as valuable intellectual property. The threat of malicious activity including data theft, Denial of Service (DoS) attacks and virus outbreaks is very real and handling incidents on this scale will require a collaborative effort.

In addition, the SANReN project is working towards enabling participation in *big science* projects such as the Large Hadron Collider (LHC) experiment and the Square Kilometre Array (SKA). Security on the network is an important factor to consider when participating in such projects.

Figure 1.2 shows the high-level architecture of the SANReN network.

1.2.2 The Tertiary Education and Research Network of South Africa

TENET was created by the public universities of South Africa to function as a vehicle for collaborative internetworking. TENET is a non-profit company whose members are the public universities and some of the science councils of South Africa (Martin, 2012). TENET essentially acts as an ISP to its members and is the operator of the SANReN network on behalf of the CSIR (Petruccione et al., 2013, p. 26).

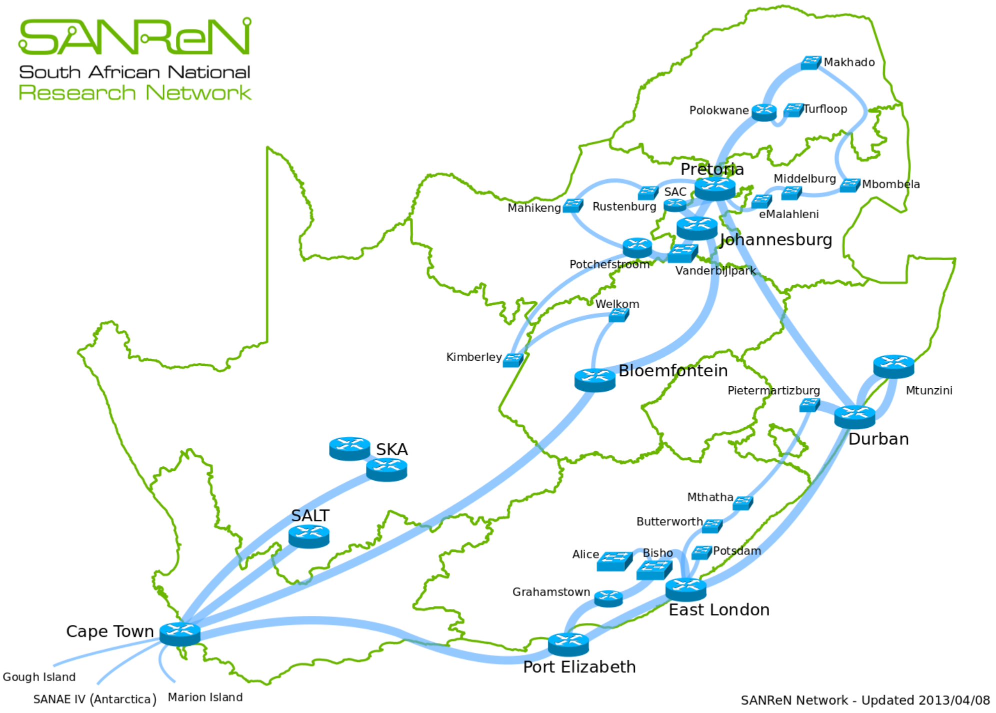


Figure 1.2: SANReN network high-level architecture
(by S. Mammen <smammen@csir.co.za>)

This unique partnership makes the South African NREN model dissimilar to that used by most other NRENs where the provider of the infrastructure also operates it. TENET and SANReN will need to work closely together in establishing a security team for the SA NREN, deciding how it will operate and who will be responsible for the management thereof, in order for it to be successful.

1.2.3 Incident response in NRENs

According to the Trans-European Research and Education Networking Association (TERENA), "most research and education networks have some sort of computer security incident handling and response team (CSIRT) for their own community" (TERENA, 2010, para. 6). Out of the 42 NRENs in Europe (van Pinxteren, 2011), 37 are listed as providing CSIRT services (ENISA, 2011; GÉANT, 2011).

Despite this best practice, the South African NREN does not currently (in 2014) provide this service. The TENET Network Operations Centre (NOC) attempts to handle security incidents on the network but a formal CSIRT (or similar team) is yet to be established[4].

[4] This is based on personal communications with TENET and inside information I have as an employee of SANReN.

1.3 Problem area

The problem area for this research centres around establishing an incident response capability for the South African NREN. This is influenced by various national and global *forces from above*; numerous guidelines, standards and best practise documents as *influencers from the side*; and the complex *situation on the ground* covering the inter-relationship between SANReN, TENET and the beneficiary institutions. A diagram of these effects is shown in figure 1.3.

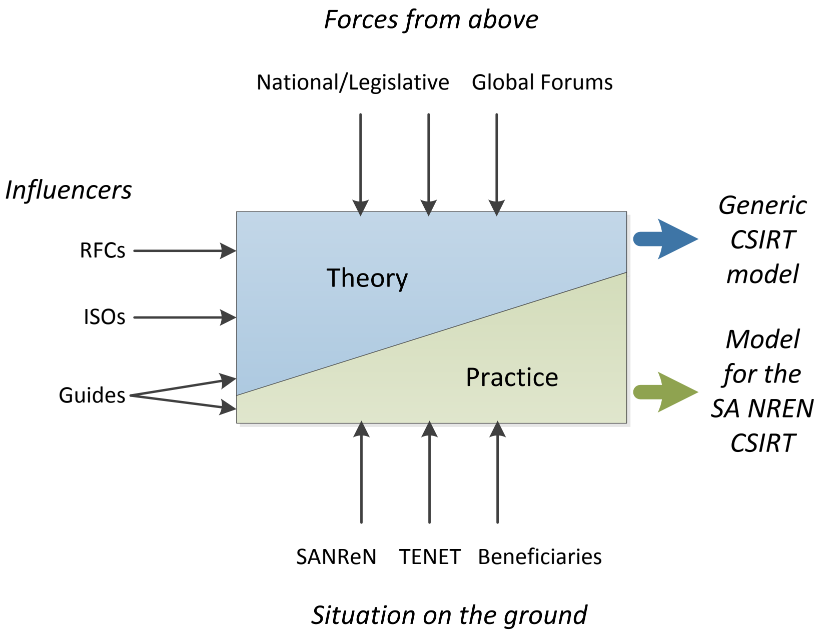


Figure 1.3: Problem area (by author)

Forces from above

These entail parties and sources over which there is no control within the scope of this research but which do influence the approach followed. These *forces* include national and legislative forces such as the proposed Cybersecurity Policy of South Africa (DoC, 2010) as well as global IT security collaboration initiatives such as the Forum for Incident Response and Security Teams (FIRST)[5] and Trusted Introducer (TI)[6].

[5] http://www.first.org

[6] http://www.trusted-introducer.org/

Situation on the ground

This covers all directly-affected and involved organisations which can be influenced and are partially controllable through the establishment process. At the same time, the structure, policies, politics and interests of these organisations must be considered during the investigation and implementation phases. The parties in this category include SANReN and TENET as well as the beneficiary institutions of the network (primarily universities and science councils).

Influencers from the side

Standards, recommended practices, guidelines and the like come in from the side. They provide useful recommendations and practices for establishing a CSIRT or similar team. The best current practice for the Internet community is documented in RFC2350 "Expectations for Computer Security Incident Response" (Brownlee & Guttman, 1998). SANS (2008) is an ISO implementation that covers IT security techniques and provides valuable insight when considering establishing an IT security team and services. Cichonski, Millar, Grance, and Scarfone (2012) provide a guide to handling computer security incidents including Incident Response Team (IRT) structures, collaboration and services. Finally, two recognised authorities providing guidelines for use when establishing a CSIRT are the Software Engineering Institute at Carnegie Mellon University (2006) and the European Network and Information Security Agency (ENISA, 2006).

These influencers and forces can be separated as shown into a "theoretical" section, applying to all CSIRTs irrespective of the environment, and a "practice" section, where the generic model is instantiated in a specific context. The influencers can alternatively be seen as the "means" or the set of available resources; the outputs as the "end goals and constraints"; forces as "laws" or uncontrollable environmental factors; and the situation on the ground as the domain of the research (Hevner, March, Park, & Ram, 2004, p. 88).

What is ultimately needed is a strategy considering inputs from all these areas to solve the problem of establishing an effective incident response capability for the South African NREN. The next section clarifies the research problems addressed by this study.

1.4 Research problems

There are a plethora of guidelines and processes to follow when setting out to establish a CSIRT and where to start is not clear. A lot of advice is provided about what aspects to consider without a consistent method or process to follow ensuring that the most important of these "requirements" for establishing a CSIRT are catered for. Therefore, the first problem addressed by this dissertation is the *lack of a clear, holistic method to follow when setting out to establish a CSIRT*.

This research will enable one to develop a model of the CSIRT for the SA NREN; the implementation of which will address *the deficiency of an incident response capability in the SA NREN environment*. Furthermore, although isolated security teams may exist within the SA NREN beneficiaries, there is *no mechanism for coordination of incident response activities*.

Not having this capability makes the NREN vulnerable as an attack target; for the NREN critical infrastructure itself, as a high-bandwidth platform for launching attacks against external targets, and as an access mechanism to valuable resources (e.g. intellectual property) housed within beneficiary (connected) institutions. At the moment, there is also *no real means of ascertaining the level of malicious activity occurring on the network*.

These problems can be summarised as

a. the lack of a definitive method for establishing a CSIRT (in general), and

b. the lack of an incident response capability in the SA NREN environment.

The need for this research is confirmed in chapter 10. The following section will present the research objectives that need to be addressed in order to solve these problems.

1.5 Research objectives

To address the research problems, this study aims *to provide a holistic, systematic model resulting in a strategy for establishing a CSIRT for the SA NREN.*

To do this, the following sub-objectives need to be met:

1. defining a CSIRT and what they provide (chapter 3);
2. exploring the CSIRT state-of-the-art (including best practices) and determining the subsequent requirements for establishing a CSIRT (see chapters 4 to 7); and
3. designing a generic model for establishing a CSIRT (chapters 8 and 9).

This model is then instantiated in the SA NREN environment by

1. evaluating the current SA NREN environment (chapter 10), and
2. applying the generic model to this environment (chapter 11).

Achieving these objectives requires a methodology which will be conferred in the following chapter. Next, the scope of this research is delineated.

1.6 Scope and delineation

The problem area provides clues as to the parameters of this research. For the purpose of scoping the study, the objectives can be re-stated as follows:

a. study *CSIRT* literature to determine the requirements for establishing a CSIRT,

b. categorise these *requirements* using *a* suitable governance/management framework,

c. identify relationships between the requirements,

d. develop a generic model for *establishing a CSIRT* based on these requirements and links,

e. survey the *SA NREN environment*, and

f. *demonstrate* utility of the model by applying it to design a *CSIRT for the SA NREN.*

The scope or domain of this study is therefore revealed as

a. *CSIRTs* (as opposed to other IRT models), and

b. *NRENs* (and specifically the *SA NREN*).

The *CSIRT* (or CERT®) model is most commonly used as the incident response mechanism in *NRENs*; it is also the most developed and documented. Although Warning, Advice and Reporting Points (WARPs) (Proctor, 2012) and the Community-orientated Security, Advisory and Warning (C-SAW) team (Ellefsen & von Solms, 2010) models may be attractive in a developing country environment, WARPs have limited implementations (UK only) and there is no known implementation of the C-SAW model. Literature from these related areas is therefore not included in the primary sources.

Only *requirements* and related decisions needed for *establishing a CSIRT* are considered. Operational or implementation-specific aspects are thus excluded from this study. This includes any pre-design (e.g. management buy-in) or post-design (e.g. sources for continual funding) considerations. Excluding these requirements assists in developing a more concise and readable model.

Only *one framework* will be used for categorising the requirements. This framework should be simple while still accommodating the primary requirement areas. Utilising additional frameworks will unnecessarily complicate the model and the development thereof.

The model will only be demonstrated in *one case*. According to design science research literature, a *single demonstration* is sufficient to show viability of new artefacts (like the *model* developed by this research) (Hevner et al., 2004, pp. 79, 84). Furthermore, the demonstration is *restricted to the design of the SA NREN CSIRT* and not its actual implementation. This is because implementation will likely take too long and be too complex for this study.

For the survey, only *security contacts* from the IT departments of institutions *actually connected to SANReN* will be targeted as respondents. These should provide a sufficient view of security incident response in the *SA NREN environment*. Finally, this environment was selected due to ease of accessibility and the existence of a known problem.[7]

Some of these limitations are addressed with ideas for future research in section 12.4 (page 226). The layout for the remainder of the dissertation is presented next.

[7] I am employed as an engineer in the SANReN CA (2014).

1.7 Layout of the dissertation

The chapter layout for this dissertation is shown in figure 1.4.

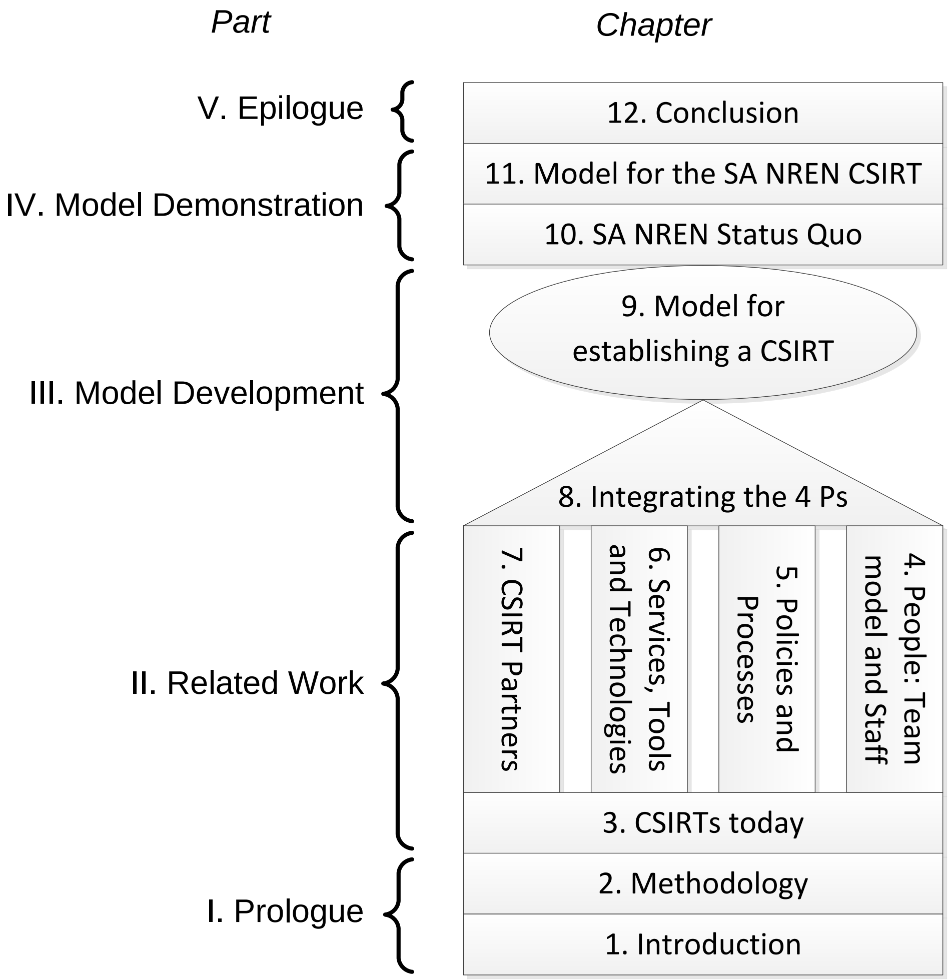


Figure 1.4: Dissertation chapter layout

Chapter 1 has introduced the domain of the discourse. The scene has been set by providing a background of modern day incident response and NRENs, defining the problem area, setting the research objective and delineating the scope of this research. How this problem will be investigated will be described in chapter 2 — Methodology. This chapter will present a design science based approach as the primary methodology to be followed for this research.

Relevant authoritative resources have been identified for the study and include standards bodies and information security or CSIRT authorities. Part II, Related Work, attempts to sanitise and present the requirements for establishing a CSIRT as extracted from these sources in a meaningful way. Chapter 3 describes CSIRTs in more detail including the basic requirements for CSIRTs as a foundation to the following chapters. Requirements from literature are presented according to ITIL's four Ps — People, Processes, Products and Partners — in chapters 4 to 7, concluding Part II.

The strength of the 4P-analysis done lies in uncovering the relationships of the four Ps to one another. The Model Development (Part III) is initiated by highlighting the relationships between the Ps in chapter 8. Chapter 9 is where the actual model development takes place by combining the information in the previous chapters to produce a model for establishing a CSIRT.

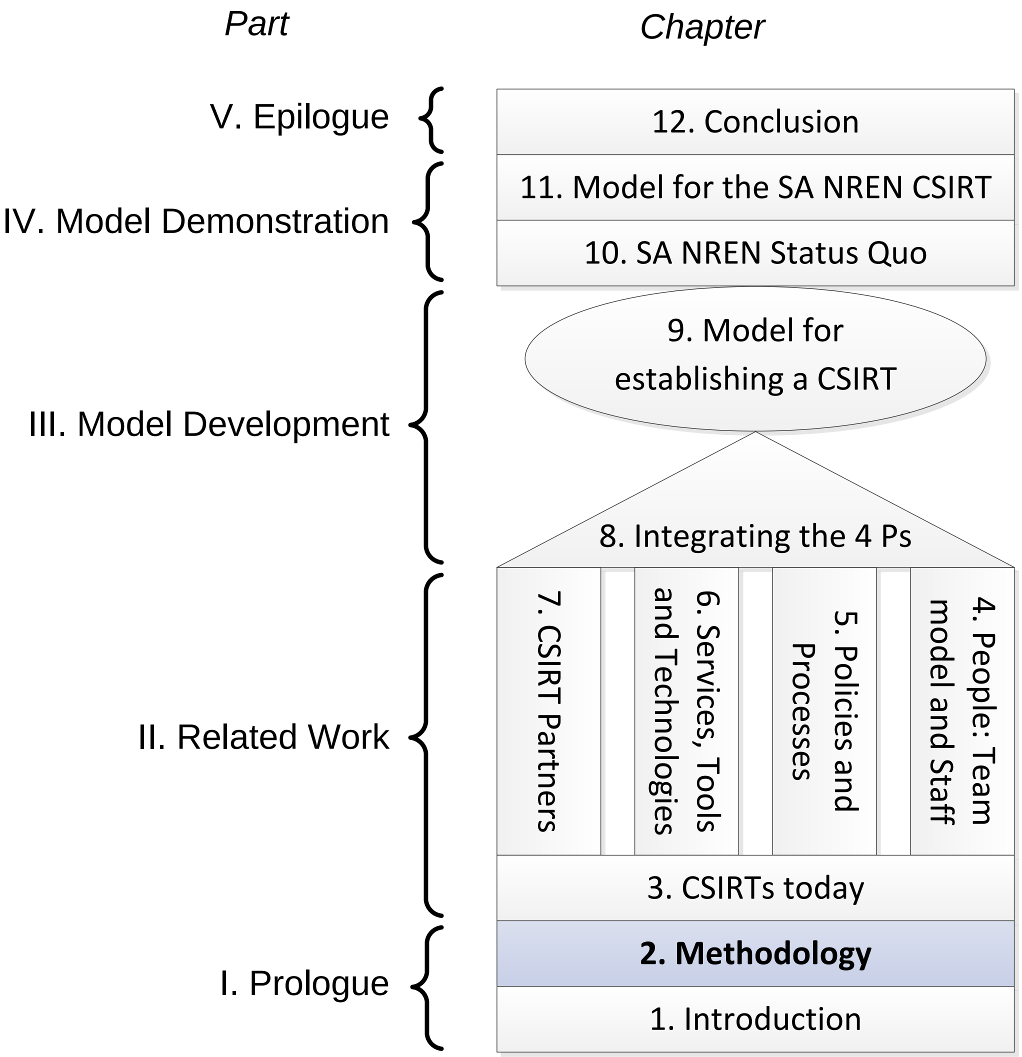
Part IV, Model Demonstration, commences with a survey performed within the SA NREN beneficiaries in chapter 10 — SA NREN Status Quo. This chapter confirms the need for a CSIRT capability and hence this research. Chapter 11 serves as an instantiation of the generic CSIRT model in the SA NREN environment, thereby demonstrating the utility of the model.

Finally, chapter 12 concludes by reflecting on the research, describing the contributions and providing suggestions for the "road ahead".

1.8 What's next?

This chapter has served as an introduction to the dissertation by providing background on IT security incidents and the modern approach to dealing with these incidents. The concept of a National Research and Education Network (NREN) has been explained as well as the nature of the South African NREN. This was followed by the problem area and research problems, together with objectives set to address these problems. The chapter layout for the remainder of the dissertation rounded off this introduction.

Next, the methodology used to approach these research problems and propose a solution will be explained.


Part
Chapter
V. Epilogue
12. Conclusion
IV. Model Demonstration
11. Model for the SA NREN CSIRT
10. SA NREN Status Quo
III. Model Development
9. Model for establishing a CSIRT
8. Integrating the 4 Ps
II. Related Work
7. CSIRT Partners
6. Services, Tools and Technologies
5. Policies and Processes
4. People: Team model and Staff
3. CSIRTs today
I. Prologue
2. Methodology
1. Introduction

Chapter 2

Methodology

> *The methodology is intended to serve as a map — guiding the research process and providing structure.*
> —Hofstee (2006, p. 107)

The previous chapter gave some background to the study by introducing mechanisms used to deal with IT security incidents as well as NRENs and the South African NREN environment. In addition, it defined the problem area and specific research problem addressed by this research. Objectives for a solution to this problem as well as a chapter layout for the dissertation were provided.

This chapter continues by explaining the methodology used to solve these problems of

a. defining a model to establish a CSIRT, and

b. realising this model through application in the SA NREN environment.

A Design Science Research (DSR) process is proposed as the methodology for this study. Design science "attempts to create things that serve human purposes" (March & Smith, 1995, p. 253). As a problem-solving paradigm (Hevner et al., 2004, p. 76), design science is well suited for providing a solution to this problem. DSR seeks to address the questions of "'What utility does the new artifact provide?' and 'What demonstrates that utility?'" (Hevner et al., 2004, p. 91).

The use of this method is further motivated by the engineering experience of the author, particularly in software design, meaning that the "build" and "evaluate" steps of DSR have a familiar feel.

2.1 Research design overview

The primary technique used for this study is *Design science Research* (DSR). It was used to create an effective artefact, a model in this instance, through the application of knowledge (March & Smith, 1995, p. 253). This knowledge was obtained via a *comprehensive study of the relevant literature* utilising a concept matrix for categorisation (Webster & Watson, 2002). DSR outputs are evaluated using criteria of value and utility: does the artefact work and (if applicable) is it an improvement over previous solutions? (March & Smith, 1995, p. 253). In order to perform this evaluation, the model needed to be "instantiated" in a suitable environment. The SA NREN was selected as this environment. A *survey* was subsequently utilised in order to solicit the required information for implementation and assess the environment as a case study.

The format of DSR products (constructs, models, methods and instantiations) suited this research particularly well. Constructs related to establishing a CSIRT are uncovered in chapters 3 to 7, forming the vocabulary of the domain (March & Smith, 1995, p. 256; Hevner et al., 2004, p. 77). These are combined to form a model, describing the task of establishing a CSIRT and expressing the relationships between the constructs (March & Smith, 1995, pp. 253, 256), in chapters 8 and 9. "The concern of models is *utility*" (March & Smith, 1995, p. 256). Therefore, this model was applied to the SA NREN environment in chapter 11, with the purpose of determining if the model works (March & Smith, 1995, pp. 254, 261). "Instantiations demonstrate the feasibility and effectiveness of the models…they contain" (March & Smith, 1995, p. 258).

The survey, used to determine the status quo with respect to malicious activity and incident response in the SA NREN environment, was implemented in the form of a questionnaire (chapter 10). Questionnaires, as with all research techniques, have their strengths and weaknesses. Relevant strengths include the ability to show correlation, choices of measurement types (ways of asking questions) (Olivier, 2008, pp. 78–84) as well as structure, facilitating quantitative analysis and volume (they can be sent to more people than interviews) (Hofstee, 2006, pp. 132–133). The last benefit, i.e. being able to distribute the survey to a large number of possible respondents in a resource-efficient manner, was particularly attractive for the purpose of this survey.

Potential weaknesses include a biased sample, ambiguous or unclear questions, difficulties in processing responses to open questions and obtaining sensitive and honest information (Olivier, 2008, pp. 80–82). These can be mitigated through proper design of the questionnaire as further elaborated on in chapter 10.

In the following section the approach used for the literature survey, as a means of extracting the relevant information from the knowledge base, is presented. This is followed by further elaboration on the DSR approach used for the remainder of the research.

2.2 The literature study

An in-depth literature study was performed as the foundation for this research. This section introduces the primary literature, presents the framework used for categorising the information and culminates in a concept matrix of the literature using this framework.

2.2.1 Summary of the literature

A comprehensive literature search was performed with the objective of determining the primary sources of CSIRT literature. Reading through the material revealed a pattern of authoritative sources from respected authors. It was found that the main institutions affiliated with these sources include the Software Engineering Institute (SEI) of Carnegie Mellon University (CMU) (Alberts et al., 2004; Killcrece et al., 2003a; Killcrece, Kossakowski, Ruefle, & Zajicek, 2003b; West-Brown et al., 2003) (who established the first CERT in 1988[1]), the European Network and Information Security Agency (ENISA) (ENISA, 2006, 2010), the National Institute of Standards and Technology (NIST) (Cichonski et al., 2012) and the SysAdmin, Audit, Networking and Security (SANS) Institute (Cichonski et al., 2012). The latest publications from these institutions were selected as the primary sources for this study[2]. In this section a brief summary of these sources are presented (alphabetically by surname of the first author).

[1] `http://www.cert.org/about/`

[2] Although some of these references may appear “dated” the foundations are still applicable and provide good academic value particularly due to the authoritative nature of the sources. The lack of updates to these publications further indicates that, most likely, nothing significant has changed to reduce their value. The most recent references were utilised where possible.

Alberts et al. (2004): Defining incident management processes for CSIRTs: A work in progress

This report takes a process-centric approach to identifying the resources and roles required for incident management. The process definitions are accompanied by workflow diagrams and descriptions. The resulting process maps provide a best-practice model outlining the "main functions and activities required for a successful incident management capability" (Alberts et al., 2004, p. 8).

Brownlee and Guttman (1998): Expectations for computer security incident response

This best current practice Request for Comments (RFC) provides a general framework for what can reasonably be expected of a CSIRT and presents the important subjects that are of concern to the community. A template for CSIRTs is provided as an aid for implementing and communicating the recommendations. Although quite old, this RFC is still used as the basis for defining many CSIRTs. This is evidenced by the hits returned of RFC 2350 descriptions when googling *cert OR csirt rfc 2350*[3], showing the relevance of RFC 2350 to this research.

Cichonski et al. (2012): Computer security incident handling guide

This guide from the National Institute of Standards and Technology (NIST) provides recommendations for establishing a successful incident response capability. Incident handling in general is also featured with the primary focus on detecting, analysing, prioritising and handling incidents.

ENISA (2006): A step-by-step approach on how to set up a CSIRT

This document, provided by the European Network and Information Security Agency (ENISA), covers business management, processes and technical aspects of CSIRT establishment. It provides information on "what a CSIRT is, what services it can provide and what the necessary steps are to get started" (ENISA, 2006, p. 4).

[3] e.g. `http://www.ren-isac.net/csirt/`, `https://www.cert.at/about/rfc2350/rfc2350_en.html`

ENISA (2010): Good practice guide for incident management

Another handbook by ENISA, this more recent guide provides practical information and good practices for managing network and information security incidents. "For a CERT in the set-up stage this guide will provide very valuable input on how to actually shape incident management and especially the incident handling service" (ENISA, 2010, p. 4).

Killcrece et al. (2003a): Organizational models for Computer Security Incident Response Teams (CSIRTs)

This handbook provides guidance on selecting the "right" model for an organisation's incident response capabilities. The handbook's primary focus is on the organisational model and operational structure of the team. Common CSIRT models with their attributes, respective advantages and disadvantages and typical service offerings are discussed.

Killcrece et al. (2003b): State of the practice of Computer Security Incident Response Teams (CSIRTs)

A comprehensive survey (distributed between June and August 2002) forms the basis of this technical report intended to "provide a view of the current state of the CSIRT practice" (Killcrece et al., 2003b, p. xii). The findings are presented in detail with a summary of what CSIRTs require to be effective. This was complemented by a literature review which includes a basic framework of "common areas that an organization should consider implementing when planning a response capability" (Killcrece et al., 2003b, p. 84) which is helpful to both new and existing CSIRTs.

Northcutt (2003): Computer security incident handling

This step-by-step publication presents an "action plan for dealing with intrusions, cyber-theft, and other security-related events" (Northcutt, 2003, p. i). It reflects the experience of incident handlers from over 50 commercial, government and educational organisations (Northcutt, 2003, p. iii) and is specifically intended to provide a starting point for incident handling procedures. An "emergency action card" is provided for organisations that are not prepared when an IT security incident occurs (Northcutt, 2003, p. x).

Penedo (2006): Technical infrastructure of a CSIRT

The goal of this paper is to provide a guide for building the technical infrastructure required by a CSIRT, with an emphasis on the necessary tools, equipment and mechanisms. The technical infrastructure of the Portuguese NREN CSIRT is used as an operational example.

Smith (1994): Forming an incident response team

Based on the author's experience of building the Australian Security Emergency Response Team (SERT), this paper looks at what it takes to form and maintain an incident response team. Topics include the constituency, policies, information, equipment and tools as well as partner relationships and interactions (Smith, 1994, p. 1).

West-Brown et al. (2003): Handbook for Computer Security Incident Response Teams (CSIRTs)

"This document provides guidance on forming and operating a computer security incident response team (CSIRT)" with a particular focus on the incident handling service (West-Brown et al., 2003, p. xv). In addition, a basic CSIRT framework is provided covering the mission, constituency, organisational placing and relationships of the CSIRT to other teams. Detailed descriptions of CSIRT services, policies and team operations (including staffing issues) are also supplied.

These papers, reports, guides and other documents range from 6 to 291 total pages with an average of 123 pages. As a result, a method to make the data more coherent and useful was required. The four Ps from ITIL seemed to suit this purpose well by providing categories for sorting the data without added complexity. While reading the literature, different colour highlighters were used for each of the Ps as well as a category for "other" (anything that looked interesting but did not quite fit into the Ps). This turned out to provide valuable information for the category of *business requirements* which matched up with ITIL's management framework quite nicely. The next section therefore, introduces ITIL's management framework followed by a concept matrix of this literature.

2.2.2 ITIL's four Ps

The IT Infrastructure Library (ITIL®) advises that the four Ps need to be aligned with the business and therefore proposes "five areas that need to be considered with regard to the design of a management architecture" (Hunnebeck, 2011, p. 61). These five areas are:

1. business requirements (objectives within the organisation),
2. people (including roles and activities),
3. processes and procedures,
4. management tools, and
5. technology.

Services (as the basis of ITIL's framework) are also important. Lastly, to complete the "four Ps", partners are included. These areas are used to present the requirements for CSIRTs resulting from the literature survey as shown in figure 2.1.

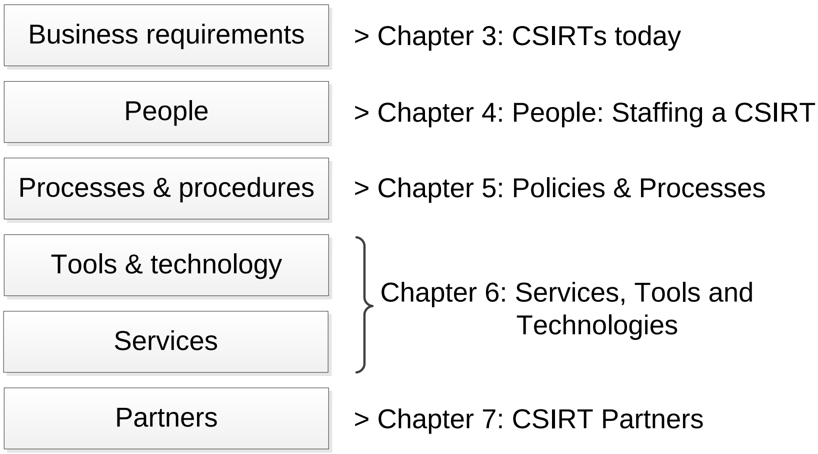

Business requirements
> Chapter 3: CSIRTs today
People
> Chapter 4: People: Staffing a CSIRT
Processes & procedures
> Chapter 5: Policies & Processes
Tools & technology
Services
Chapter 6: Services, Tools and Technologies
Partners
> Chapter 7: CSIRT Partners

Figure 2.1: Presenting the requirements for CSIRTs (by author)

2.2.3 Concept matrix

The previous two sections were brought together through the use of a concept matrix to synthesise the literature (as recommended by Webster and Watson (2002)). This resulting matrix is shown in table 2.1. Primary sources are shown using double ticks (✓✓) in the table. More detailed concept matrices (showing the subsections under each of the requirement categories) are available in appendix B (page 232).

Table 2.1: Literature concept matrix

	Business requirements	People	Policies & Processes	Services	Tools & Technologies	Partners
Alberts et al. (2004)	√	✓✓	✓✓	√	✓	✓
Brownlee and Guttman (1998)	✓		√	✓	✓	✓
Cichonski et al. (2012)	✓	✓	✓	√	✓	✓
ENISA (2006)	✓✓	✓✓	✓✓		✓	√
ENISA (2010)	✓✓	✓	✓✓	✓	✓✓	✓
Killcrece et al. (2003a)	✓	✓✓	✓	✓✓	✓	✓
Killcrece et al. (2003b)	✓	✓✓	✓✓	✓	✓✓	✓
Northcutt (2003)		✓	✓		✓	✓
Penedo (2006)					✓✓	
Smith (1994)	✓	✓	✓✓	√	✓	✓
West-Brown et al. (2003)	✓	✓	✓✓	✓✓	✓✓	✓

√= minimal information or reference only; ✓= useful information; ✓✓= primary source

Alberts et al. (2004), with their process-centric focus, came out as a primary reference for people and processes. The ENISA guides are both strong on CSIRT business requirements as well as policies and processes. Respectively, people (ENISA, 2006) and tools and technologies (ENISA, 2010) also came out strong. The focus on organisational models is apparent with Killcrece et al. (2003a) shown as a primary source for people requirements. This is complemented by detailed service descriptions including applicable and appropriate services for each model and hence the emergence as a primary reference for services. As can be expected from a state of the practice survey and general discussion on CSIRTs, the strengths are broader for Killcrece et al. (2003b). The handbook from West-Brown et al. (2003) is similarly diverse with strengths in multiple categories. Penedo (2006) is clearly focused on tools and technologies in line with the goal of the paper. Lastly, although broad strengths would be expected from Smith (1994) (considering the title and topics of the paper) it appears to be stronger in policies and processes than the other categories.

Moving on from the literature study, the next section details the primary method used as the framework for this research. Design science research is introduced followed by detailed explanations of the DSR framework, guidelines and process selected for this study.

2.3 Design Science Research (DSR)

Design Science (DS) has been defined as creating and evaluating artefacts "intended to solve identified organisational problems" (Hevner et al., 2004, p. 77). This emphasises the two basic activities of *building* and *evaluating* artefacts (March & Smith, 1995, p. 254). Ideally, these artefacts should be new and innovative, extending the boundaries of human and organisational capabilities (Hevner et al., 2004, p. 75).

Four types of IT artefacts for design science have been defined in literature: constructs, models, methods and instantiations (Hevner et al., 2004, p. 77). A *model*, as a representation of the solution space to a problem (Hevner et al., 2004, p. 78), is the primary deliverable of this dissertation. A secondary artefact, an implementation of this method in a real world context, is further provided as a demonstration of the model. This *instantiation* demonstrates viability, "enabling concrete assessment of an artifact's suitability to its intended purpose" (Hevner et al., 2004, p. 79).

The basic process of *build* and *evaluate* has been borrowed from design science research for this study (Hevner et al., 2004, pp. 79–80). An artefact is built to address a specific problem and evaluated according to its effectiveness as a solution. The process allows for re-iteration if necessary until a suitable solution is obtained (Hevner et al., 2004, p. 78).

2.3.1 A framework for DSR

A framework for understanding, executing and evaluating Information Systems (IS) research has been proposed by Hevner et al. (2004, p. 80). This framework is a good fit for our research as it utilises a design-science approach with behavioural-science theory (Hevner et al., 2004, p. 79). Figure 2.2 shows the adapted framework, with relevant chapters, for this research.

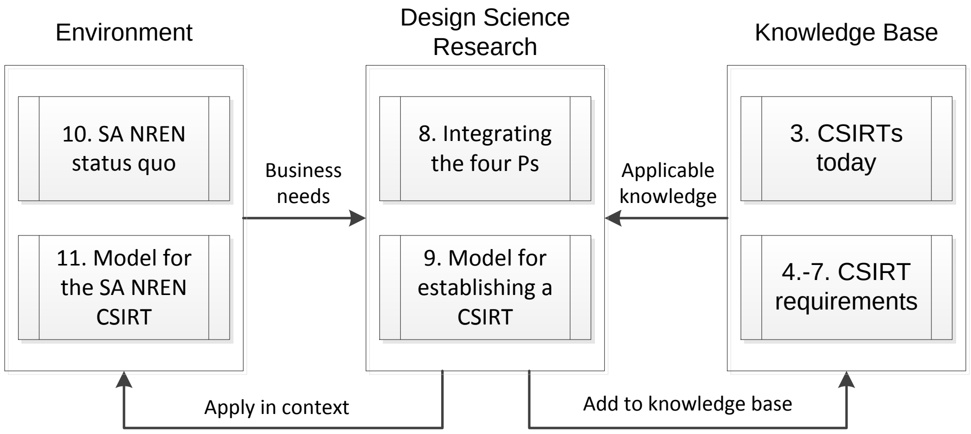


Figure 2.2: Framework for this research (based on Hevner et al. (2004, p. 80))

The IS environment, consisting of people, organisations and technology, is similar to the four Ps identified for presenting the requirements for CSIRTs. Furthermore, “framing research activities to address business needs assures research relevance” (Hevner et al., 2004, p. 79). Thus, the application of the DSR artefact in the SA NREN environment as shown in the figure.

2.3.2 A process for DSR

A process for executing and presenting design science research has been developed by Peffers, Tuunanen, Rothenberger, and Chatterjee (2007). The idea was to highlight the outputs expected from DSR using a consensus-building approach based on prior literature (identifying common elements from seven key papers) (Peffers et al., 2007, p. 52). "For DS research, a methodology would include three elements: conceptual principles to define what is meant by DS research, practice rules, and a process for carrying out and presenting the research" (Peffers et al., 2007, p. 49).

The process was designed according to these three objectives (Peffers et al., 2007, pp. 46, 50):

1. Build upon previous (influential) literature.

2. Produce a nominal process for performing DS research.

3. Provide a template for presenting and evaluating DSR.

Finally, the process was demonstrated and shown to satisfy these objectives through evaluation in four case studies (Peffers et al., 2007, pp. 57–70). These studies did not specifically use the proposed DSR process (as it was not yet available) but the process was successfully mapped to them in retrospect, illustrating its fit and utility. The case studies were further selected to illustrate how different points of entry for the research fit into the process (each of the case studies had a different entry point) (Peffers et al., 2007, p. 72) and to provide a scope of four different research problems for the demonstration (Peffers et al., 2007, p. 74). The outcome was a formal research framework useful for performing DSR as adapted in this study. The process consists of the six activities shown and defined in table 2.2.

It has been argued that instantiation of an artefact demonstrates both feasibility of the design process as well as of the product (Hevner et al., 2004, p. 84). Hevner et al. (2004, p. 84) argue further that prototype demonstration in a research or single organisational setting (as in this case) is a necessary first step towards deployment. Therefore, for this study, it was decided to combine the demonstration and evaluation steps as shown in figure 2.3. This effectively means that the demonstration (as an "instantiation" of the artefact) serves as a proof of concept in the SA NREN environment.

How this dissertation is mapped to this process (as the *methodology* used for this research) is shown in figure 2.4.

Table 2.2: Design science research process (Peffers et al., 2007, pp. 52–56)

	Activity	Description
1	Define the problem	Identify the specific research problem and why a solution is needed.
2	List solution objectives	Specify how a new artefact supports a solution or how an existing one will be an improvement.
3	Design and develop	An artefact (construct, model, method or instantiation)
4	Demonstrate	Solve the problem in a suitable context (by "experimentation, simulation, case study, proof" or similar (Peffers et al., 2007, p. 55)).
5	Evaluate	Observe and measure the effectiveness and efficiency of the artefact.
6	Communicate	Through publication (for example)

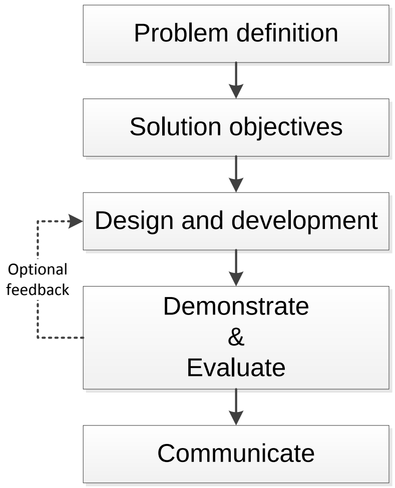


Figure 2.3: Design science research process
(adapted from Peffers et al. (2007))

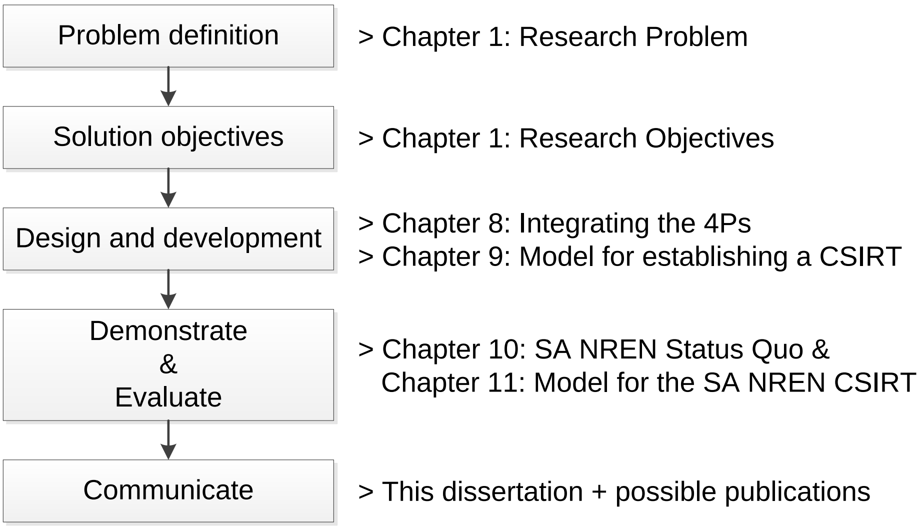

Problem definition
> Chapter 1: Research Problem
Solution objectives
> Chapter 1: Research Objectives
Design and development
> Chapter 8: Integrating the 4Ps
> Chapter 9: Model for establishing a CSIRT
Demonstrate & Evaluate
> Chapter 10: SA NREN Status Quo & Chapter 11: Model for the SA NREN CSIRT
Communicate
> This dissertation + possible publications

Figure 2.4: Design science research process mapping to chapters (by author)

2.3.3 Guidelines for DSR

Seven guidelines have been proposed for understanding, executing and evaluating design science research (Hevner et al., 2004, pp. 82–90). Peffers et al. (2007, p. 49) refer to these as "practice rules" for DSR. These guidelines are shown in table 2.3 and will be adhered to in this research.

Table 2.3: Design science research guidelines (Hevner et al., 2004, pp. 82–83)

Guideline 1:	Design as an artefact
Guideline 2:	Problem relevance
Guideline 3:	Design evaluation
Guideline 4:	Research contributions
Guideline 5:	Research rigour
Guideline 6:	Design as a search process
Guideline 7:	Communication of research

2.4 Conclusion

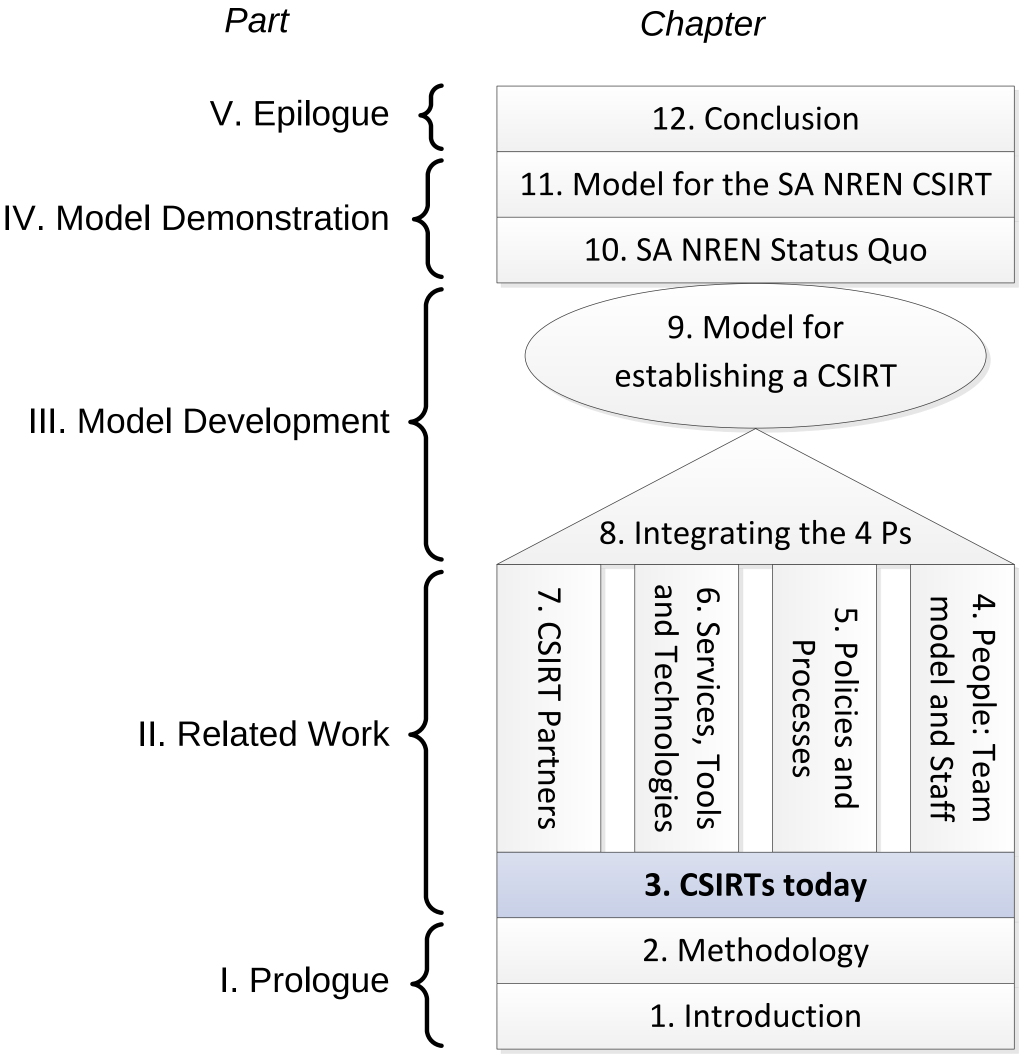
This chapter described the methodology used for this research commencing with an overview of the research design. Design science research was revealed as the primary technique used with a comprehensive literature study as the foundation. A survey was utilised to extract information needed for demonstrating the DSR model in the SA NREN environment.

Subsequent sections elaborated on the study of the literature and design science research approach. The literature study section summarised the key literature and included a concept matrix for categorisation according to the four Ps of ITIL (plus business requirements and services). The DSR section presented a framework, process and guidelines for DSR according to recognised papers on the topic. How these were utilised in the research was described, including mapping of the work to each section of the framework and process activity as applicable.

The next chapter marks the beginning of Part II of the dissertation covering the work related to this research. This is achieved by discussing CSIRTs today with a specific focus on the requirements for CSIRTs.

Part II

Related Work


Part
Chapter
V. Epilogue
12. Conclusion
IV. Model Demonstration
11. Model for the SA NREN CSIRT
10. SA NREN Status Quo
III. Model Development
9. Model for establishing a CSIRT
8. Integrating the 4 Ps
II. Related Work
7. CSIRT Partners
6. Services, Tools and Technologies
5. Policies and Processes
4. People: Team model and Staff
3. CSIRTs today
I. Prologue
2. Methodology
1. Introduction

Chapter 3

CSIRTs today

> *"Every single country that is connected to the internet must have the capability to effectively and efficiently respond to information security incidents. CERTs are able to do much more."*
>
> —ENISA (2010, p. 8)

There are a number of ways in which the Internet community has adapted to dealing with incidents resulting from the threats mentioned in Chapter 1. Ultimately, all of these response mechanisms involve *people* in some sort of team structure and collaboration: individuals cannot fight alone. CSIRTs, as the chief response mechanism, were introduced in section 1.1.2.

Similar to the way in which an NREN typically provides value-added services on top of the network, CSIRTs are able to do far more than just respond to IT security incidents. They provide security services to diverse communities and can even facilitate education and training (ENISA, 2010).

This chapter will describe CSIRTs in more detail, including a high-level overview of the requirements for CSIRTs. The chapters proceeding this will describe the requirements in detail, utilising a structured approach according to the methodology, before moving on to defining a model for establishing a CSIRT.

3.1 Background

A Computer Security Incident Response Team (CSIRT) (or Computer Emergency Response Team (CERT®)) is a group of IT security experts primarily responsible for handling security incidents in an IT environment. These include all kinds of malicious activity on a network and PC level, ranging from Denial of Service (DoS) attacks and hacking attempts to malware and compromised systems. A CSIRT attempts to isolate, mitigate the effects of, disable and assist with recovery from these incidents. Secondary responsibilities may include incident prevention, advisory dissemination and security consultancy services in order to minimise risk and reduce actual incidents. The exact services provided depend on the needs of the constituency (customer base) and the available resources (finances and staff) (ENISA, 2006). A CSIRT was thus defined in Chapter 1 as:

> *"an organization or team that provides services and support to a defined constituency for preventing, handling, and responding to computer security incidents"* (Alberts et al., 2004, p. 1).

The team can be formalised or called together on an ad hoc basis as needed (Killcrece et al., 2003b). In addition, a CSIRT can coordinate incident response activities between groups or organisations (Killcrece et al., 2003a).

CSIRTs can operate in a hierarchy coordinated by global and regional forums. Then there are national CSIRTs followed by sector CSIRTs and finally individual company or organisational CSIRTs. This hierarchy is shown in figure 3.1 (supplementing West-Brown et al. (2003, pp. 20–21)). The dashed lines represent possible "bypassing" of the ideal hierarchy in special situations (e.g. the coordinating CSIRT is yet to be established, sector CSIRTs collaborating with peers in other countries, etc.).

3.1.1 Challenges when establishing a CSIRT

Grobler and Bryk (2010) present a number of challenges faced through the authors' experience of establishing a national CSIRT in a developing country. Most of the challenges are also relevant when establishing other kinds of CSIRTs. These challenges are identified in table 3.1.

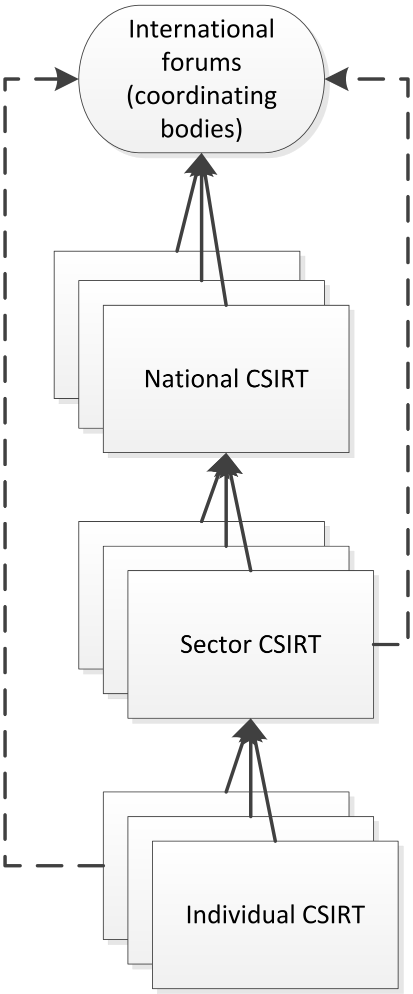


Figure 3.1: The CSIRT hierarchy (by author)

Table 3.1: Challenges when establishing a CSIRT (Grobler & Bryk, 2010)

Step	Challenge
Clarify mandate & policy issues	Unclear mandate/mission Ill-defined roles and responsibilities
Obtain management support	Lack of management support Bad publicity
Secure funding	Finding investments
Find available resources	Amount of equipment required Restrictive host organisation policies
Business plan	Determining service hours Insufficient staff (numbers) Selecting a revenue model Choosing the CSIRT services
Document operational & technical procedures	Understanding the processes Untested procedures which may fail
Commence operations	Interacting with the constituency and external parties

Challenges related to the specific environment (e.g. cultural differences) as well as those directly related to CSIRT implementation (e.g. project delays) were deliberately excluded from this list as they are outside of the scope of this research. A lack of funding, management support, trained incident handling staff and a clearly defined mission and authority were confirmed as CSIRT challenges by Killcrece et al. (2003b). This shows that not all challenges are unique to the developing country environment.

Alternative approaches to incident response teams have been proposed to address some of these challenges. These include Warning, Advice and Reporting Points (WARPs) (Proctor, 2012) and the Community-orientated Security, Advisory and Warning (C-SAW) team (Ellefsen & von Solms, 2010). How this research addresses these challenges is discussed in the concluding chapter.

CSIRT services are considered next, commencing the foundation for the CSIRT model.

3.1.2 CSIRT Services

CSIRT services are classified in three broad categories, namely reactive, proactive or security quality management services (Killcrece et al., 2003a). A commonly accepted list of services is provided in table 3.2. Reactive services involve actions taken to resolve or mitigate incidents as they occur (Alberts et al., 2004). These are the core CSIRT services (Killcrece et al., 2003a). Proactive services are aimed at preventing incidents from occurring in the first place through securing systems, providing training and education, monitoring and sharing information (Alberts et al., 2004). Security quality management services are "well-known, established services designed to improve the overall security of an organisation" and are not necessarily CSIRT-specific (Killcrece et al., 2003a, p. 22). To be effective, services should address a range of reactive and proactive issues (West-Brown et al., 2003). More detail on CSIRT services is provided in section 6.1.

Table 3.2: CSIRT services (adapted from ENISA (2010, p. 26))

Reactive services	Alerts and warnings Incident handling Vulnerability handling Artefact handling
Proactive services	Announcements Technology watch Security audits or assessments Configuration and maintenance of security tools, applications and infrastructure Development of security tools Intrusion detection services Security-related information dissemination
Security quality management services	Risk analysis Business continuity and disaster recovery planning Security consulting Awareness building Education and training Product evaluation or certification

3.2 Requirements for establishing a CSIRT

Successfully providing CSIRT services requires an holistic approach. “Policies, procedures, equipment, premises, contacts, and staff should be established before commencing operations” (Smith, 1994, p. 32). The author argues though that it is more likely that many of these items will be missing or inadequate (Smith, 1994). To address this problem, a method based on the four “Ps” suggested by the IT Infrastructure Library (ITIL) namely, People, Processes, Products and Partners, is proposed. Considering that a CSIRT can be seen as a team providing specialised IT services to defined customers (the constituency) (West-Brown et al., 2003), ITIL as a framework for IT service management, and consequently the four Ps, is certainly applicable.

This section commences with defining some basic requirements for a CSIRT. In addition, the “four Ps” structure used for the remaining requirements is presented, followed by a description of CSIRT constituencies to complete the list of basic requirements.

3.2.1 Business requirements

The primary business requirements or organisational inputs that need to be considered when establishing a CSIRT are described in this section.

Environment

The CSIRT environment can be defined by the sector which will be served by the CSIRT as well as the geographic region of operations (Cichonski et al., 2012, p. 47). The sector or “business area” (Killcrece et al., 2003a, p. 3) options are shown in table 3.3. As noted by ENISA (2006, p. 10), a team may serve more than one sector, with subsequent impact on the scope of the constituency. How these different types of CSIRTs typically fit into the CSIRT hierarchy (figure 3.1) are shown in figure 3.2.

The existing organisational structure of the hosting organisation (if any) is regarded as part of the environment. The organisational requirement will determine whether the CSIRT will be established as an independent entity, embedded in an existing organisation, distributed between campuses and/or consist of volunteers from the community (ENISA, 2006, pp. 21–24).

Table 3.3: CSIRT sectors and types (based on ENISA (2006, pp. 8–10))

Type / Sector	Serving
National	Whole country (usually in a coordinating/ intermediary role)
Academic Sector	Research and education organisations
CIP/CIIP Sector	Critical Information and/or Infrastructure Protection (energy, transportation, critical ICT infrastructure, etc.)
Government Sector	Government agencies (and sometimes citizens)
Military Sector	Military departments
SME Sector	Small and medium enterprises or special interest groups (usually self organised)
Commercial	Commercial services to paying clients
Internal	Hosting organisation only
Vendor	Specific hardware or software vendor (also called a Product Security Incident Response Team (PSIRT))
Other	Any type or sector not fitting into the above

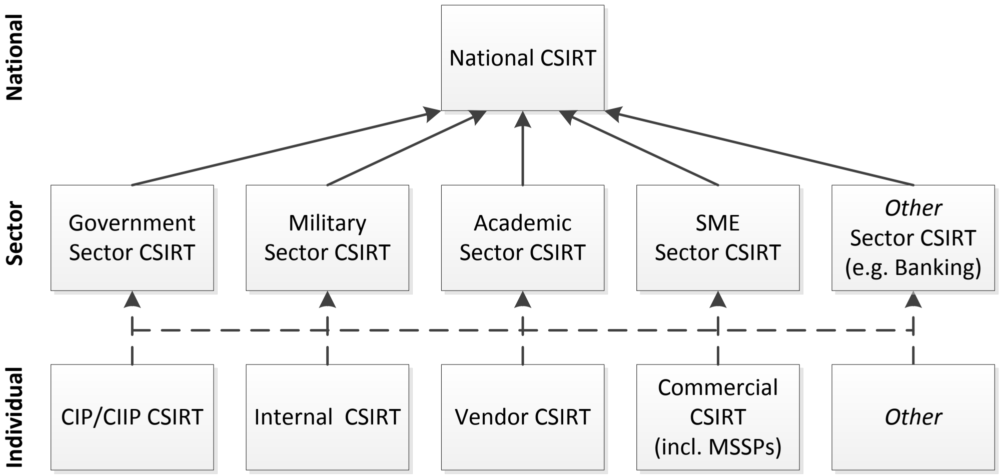


Figure 3.2: How the sectors map to the CSIRT hierarchy (by author)

Thus, the environment comprises the CSIRT sector, geographic area and organisational structure. The environment reveals the constituency and provides input to the CSIRT team model and services.

Some questions related to the organisational environment include the following (ENISA, 2006, pp. 21–24):

- Will the CSIRT be established as an independent entity with its own management and employees? >*independent* model
- Will it be embedded within an existing organisation? >*embedded* model
- Will it be distributed between independent campuses? >*campus* model
- Will it consist of volunteers from the community? >*voluntary* model

The answers to the above questions will influence the decisions made in the following chapters.

Constituency

The constituency is defined as:

> *"the group of users, sites, networks or organisations served by the team"* (Brownlee & Guttman, 1998, p. 17).

The constituency must be defined clearly and early on (ENISA, 2006). This is important because the people served by the CSIRT need to know that they have one and the team needs to know who it is serving (Smith, 1994). "Other IRTs also need to know where the boundaries of the constituency are defined so that they can direct appropriate queries to the correct team" (Smith, 1994, p. 4). A constituency can either be internal (within the same organisational structure as the CSIRT) or external; centralised or distributed (across cities, countries or even time zones) (Killcrece et al., 2003a). The constituency can be as broad as a whole region or country or as narrow as a single branch of an organisation to any other logical grouping. Government, banking and research and education network beneficiaries are examples of constituencies served by sector-specific CSIRTs (Killcrece et al., 2003b).

To identify the constituency, the CSIRT environment (or industry sector) and geographic region is determined (Cichonski et al., 2012, p. 47).

Thereafter, the constituency can be defined by (ENISA, 2010, p. 14)

- IP address range,
- domain name,
- autonomous system number(s), and/or
- free text.

IP address range, domain name and free text are most often used by research and education CSIRTs; AS number(s) are typically used by ISP CSIRTs (ENISA, 2010, p. 15). Free text is clear but can make it difficult to determine if a host (identified by IP address) is in fact part of a specific constituency or not.

Active, reliable and trusted contacts should be established as soon as the constituency is defined (ENISA, 2010). Refer to Smith (1994, p. 5) for an idea of how to go about this.

Funding

Funding has been highlighted in section 3.1.1 as a challenge when establishing a CSIRT. The available budget influences the resources that can be utilised by the CSIRT — especially people. Funding considerations can be divided into sources of income and sources of expenditure. Costs are primarily determined by the hours of operation and staff salaries (ENISA, 2006, p. 18).

More specifically, *costs* can be split between

- start-up equipment and infrastructure,
- staff salaries and benefits, and
- operational expenditures and personnel costs (Killcrece et al., 2003b, pp. 53–54).

Revenue models include the use of

- existing resources,
- membership fees,
- a project subsidy, and/or
- charging for services on a per-use basis (ENISA, 2006, p. 19).

More detailed funding strategies for CSIRTs are available from Killcrece et al. (2003b, p. 54). They also found that most CSIRTs are funded by a parent organisation (e.g. university, NREN or government).

Legal considerations

The CSIRT should be sensitive to local laws and regulations which may include specific requirements for reporting and confidentiality (Brownlee & Guttman, 1998, p. 12). An awareness of laws in other countries, with which the CSIRT cooperates, is also useful (ENISA, 2010).

CSIRTs should be aware of laws related to (Killcrece et al., 2003b; ENISA, 2006):

- telecommunications and IT services,
- data protection and privacy,
- evidence handling,
- data retention, as well as
- notification requirements (e.g. law enforcement, national CSIRT).

The specific laws relevant to the CSIRT will depend on the CSIRT environment and could include statutory and common or case laws (Killcrece et al., 2003b, p. 112). More information on legal issues is available in West-Brown et al. (2003, p. 51-58) and Smith (1994, pp. 11–12).

Authority

"Authority describes the control that the CSIRT has over its own actions and the actions of its constituents related to computer security and incident handling activities" (Killcrece et al., 2003a, p. 37).

There are four types of authority relationships that a CSIRT can have over its constituency (West-Brown et al., 2003, p. 15):

1. full — the CSIRT can undertake any actions or decisions on a constituent's behalf;
2. shared — the CSIRT can influence the decision-making process;
3. indirect — the CSIRT can exert pressure on a constituent (e.g. an ISP can disconnect services if actions are not taken); or
4. none — the CSIRT can only advise but not enforce actions.

The level of authority should be supported by management and clearly conveyed to the constituency (Killcrece et al., 2003a, p. 38). It has been argued that the lower the CSIRT authority, the *more likely* it is that constituents will report incidents and seek assistance (Smith, 1994, p. 9). Note that it is not possible to provision some CSIRT services, e.g. incident tracing and intrusion detection, without some level of authority.

The groups of business requirements identified in this section are shown in figure 3.3.

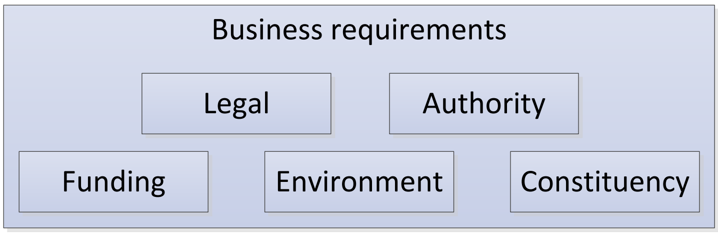


Figure 3.3: CSIRT business requirements (by author)

3.2.2 People, Processes, Products and Partners

According to ITIL, IT service management should include preparing and planning "the effective and efficient use of the four Ps" (Hunnebeck, 2011, p. 40). The four Ps localised to the CSIRT environment (based on ITIL's descriptions) include

- people — the staff and management of the CSIRT;
- processes — CSIRT policies and procedures;
- products — customer-facing services, technologies and tools; and
- partners — internal (those present in the same host organisation/ business e.g. human resources or public relations) and external (vendors, suppliers, other CSIRT teams, media, law enforcement, service providers, etc.).

To complete the picture, the constituency, or customer base (ENISA, 2006), of the CSIRT (as the consumer of the services provided) must be included.

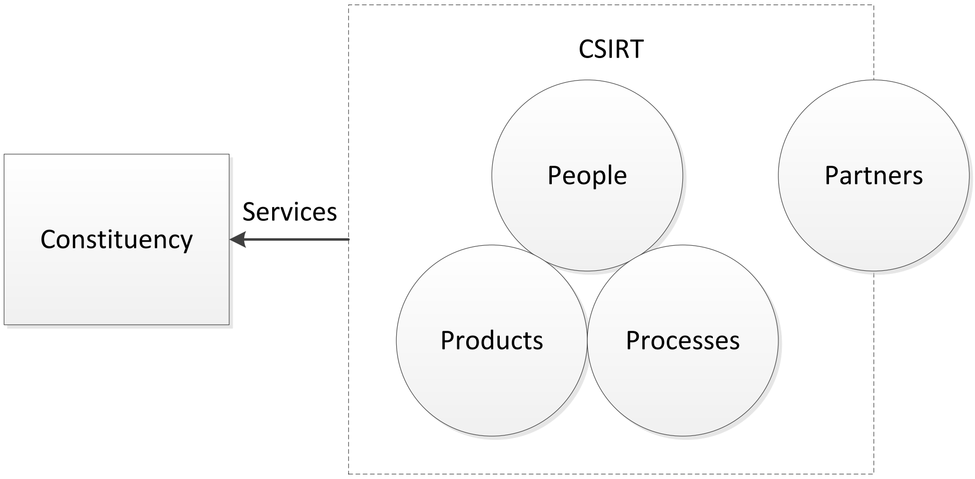


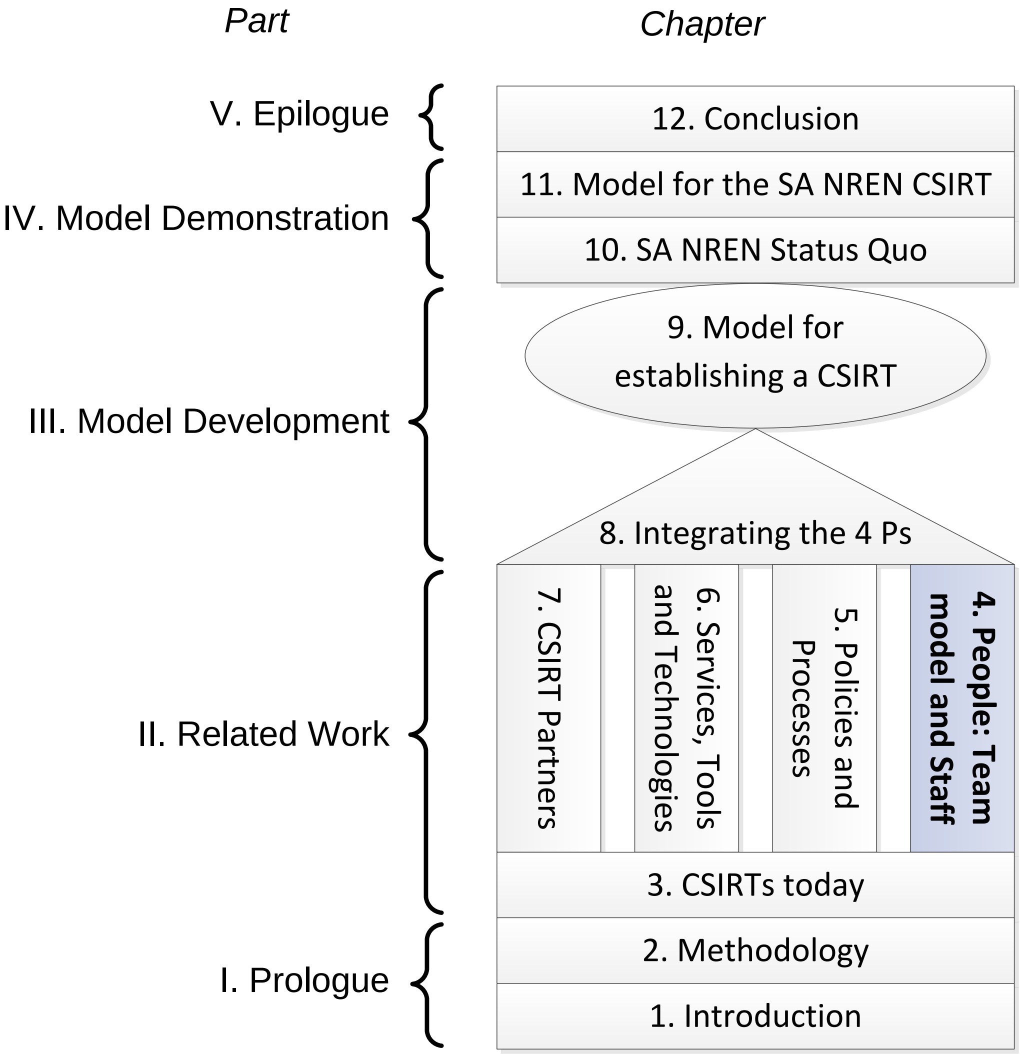
Figure 3.4: ITIL's four Ps, the CSIRT and the constituency (by author)

How the CSIRT (represented through the four Ps) and the constituency fit together is shown in figure 3.4. Partners may form part of the CSIRT depending on whether or not they assist directly with provisioning the CSIRT services (e.g as expert consultants, help desk staff, etc.).

3.3 Conclusion

This chapter has provided some background on CSIRTs: introducing the concept, some challenges when establishing a CSIRT and typical services provided by CSIRTs. The basic requirements for a CSIRT were discussed next. These include the environment, constituency, funding, legal considerations and authority of the CSIRT. The final section introduced the structure used for presenting the remaining requirements in the following chapters.

Chapter 4 will investigate people aspects focusing on the team model and staffing requirements for a CSIRT. The next chapter, chapter 5, looks at CSIRT policies and processes. Requirements for CSIRT services, tools and technologies are explored in chapter 6. Finally, chapter 7 completes the requirements by uncovering the internal and external partners involved in CSIRT activities.


Part
Chapter
V. Epilogue
IV. Model Demonstration
III. Model Development
II. Related Work
I. Prologue
12. Conclusion
11. Model for the SA NREN CSIRT
10. SA NREN Status Quo
9. Model for establishing a CSIRT
8. Integrating the 4 Ps
7. CSIRT Partners
6. Services, Tools and Technologies
5. Policies and Processes
4. People: Team model and Staff
3. CSIRTs today
2. Methodology
1. Introduction

Chapter 4

People: Team model and Staff

> The core of a team: *"People who work together to achieve a common objective."*
>
> —Cannon (2011, p. 22)

People are central to CSIRT operations. Without staff and management it is impossible to provide incident response services. "People assets represent an organisation's capabilities and resources. If capabilities are the capacity for action, people assets are the actors" (Cannon, 2011, p. 382). People also have defined roles (Hunnebeck, 2011, p. 23).

Due to the diversity of incident management across organisations, Alberts et al. (2004, p. 1) argues that defining a standard staff structure for CSIRTs is difficult. However, the team and staffing models must still be determined when establishing an incident response capability (Cichonski et al., 2012, pp. 14–15). To achieve this, the unique situation, environment and requirements of an organisation must be considered (Killcrece et al., 2003a). Related factors include the need for 24x7 availability, full- or part-time staff, staff expertise, cost and employee morale (Cichonski et al., 2012, pp. 14–15). When determining staff requirements, the following factors should be considered:

- working hours, which impact staff numbers (ENISA, 2006);
- the size, diversity and expectations of the constituency (Killcrece et al., 2003a; Smith, 1994);
- organisational structure, which determines task and responsibility allocations (Killcrece et al., 2003a); and
- burnout, which can be counteracted by providing training opportunities and time for other interests (Cichonski et al., 2012; Smith, 1994).

This chapter continues by discussing the team model, staffing model, staff numbers, work schedules, roles and responsibilities, and skills of people required for establishing a CSIRT.

4.1 Team model

ITIL notes that "team members can be co-located, or work in multiple locations and operate virtually" (Hunnebeck, 2011, p. 22). Aligned with this, CSIRT literature reveals that the team is typically structured independently (with its own management and employees), embedded within an existing organisation, distributed between institutions and/or using volunteers from the constituency (ENISA, 2006, pp. 21–24).

The selected team model depends on the existing structure of the hosting organisation (if any), the nature of the constituency and the accessibility of skilled experts (ENISA, 2006). Popular team models include the following:

Central

In this model, the CSIRT is centrally located, fully staffed and provides a single point of contact dedicated to IT security of the organisation (Killcrece et al., 2003a). This model is usually implemented in small organisations or those with limited geographic distribution (Cichonski et al., 2012, p. 13).

Distributed

This is essentially a "virtual" CSIRT — the team is made up of exisiting, distributed (usually geographically) staff reporting to a central CSIRT manager (Killcrece et al., 2003a). It is more suited to large organisations or those with distributed computing resources (Cichonski et al., 2012, p. 13). Staff may be dedicated or have additional responsibilities besides CSIRT activities (Killcrece et al., 2003a).

Coordinating

A coordinating CSIRT is a kind of "CSIRT for CSIRTs" usually providing advice without authority (Cichonski et al., 2012, p. 13). This kind of CSIRT typically has a broader scope and a more diverse constituency; it "coordinates and facilitates the handling of incidents across a variety of external or internal organizations" (Killcrece et al., 2003a, p. 34).

A team may find that it is best realised by some combination of the above (Killcrece et al., 2003a). For example, the central and distributed models can be combined. There are numerous advantages to this approach including maximising staff utilisation in strategic locations, though Killcrece et al. (2003a, p. 96) caution that the combined model "works best for very large distributed organizations or constituencies".

4.1.1 Staffing model

Full-time or part-time staffing models are the most common among CSIRTs (ENISA, 2010). Full-time staff are devoted to incident handling activities whereas part-time or ad hoc staff are typically assembled when an incident occurs (Killcrece et al., 2003b). Cichonski et al. (2012, p. 14) highlight that part-time staff should be considered when there is limited organisational funding, staff or need for incident response services. There is a risk of conflict of interest occurring though, due to team members having other obligations (ENISA, 2010).

Some alternatives to the full-time and part-time models are exchange programmes, internships (a good way to find potential new employees), volunteering and outsourcing (ENISA, 2010, pp. 22–25). Cichonski et al. (2012) build on this by indicating that staff can by partially outsourced or fully outsourced as an alternative to the employed model; what needs to be taken into account is that outsourced experts may possess deeper security or system knowledge but internal staff will be more familiar with the organisational environment.

4.1.2 Staff numbers

Literature have varying views on the number of staff required for a CSIRT. Part of the reason is that the workload and demand for incident response actions from the constituency is initially unknown (Smith, 1994). In addition, the size and diversity of the constituency has a direct correlation on the size of the CSIRT team (Killcrece et al., 2003a). In a survey conducted by Killcrece et al. (2003b, p. 70) no specific staffing trend or best practice levels were found among CSIRTs. Futhermore, a direct correlation was found between CSIRT staffing and the team's mission, funding and availability of expertise, as well as services and capabilities in the parent organisation.

Smith (1994, p. 7) argues that “Determining the appropriate number of staff to employ is a fine balance between the expected (and probably as yet, unknown) workload, and the budget constraints”. Furthermore, the team should also have sufficient capacity to deal with large and complex incidents, thereby meeting constituency expectations (Smith, 1994).

The following key values for technical staff requirements are presented by ENISA (2006, p. 24) in full-time equivalents (FTEs):[1]

- incident handling and advisory distribution — four FTEs;
- full service during office hours (including system maintenance) — six to eight FTEs; or
- fully staffed, 24x7 CSIRT — a minimum of 12 FTEs.

Due to the bursty nature of incidents, Smith (1994, p. 8) suggests having “trusted staff from other institutions on standby who could lend technical assistance in times of emergencies”. This can also help limit the effect of the unpredictability of initial staffing requirements. Finally, staffing level changes can be recommended following the evaluation of response actions; i.e. as incidents occur and response effectiveness is evaluated (Alberts et al., 2004).

4.1.3 Work schedule and hours of operation

A work schedule must differentiate between normal and after hours including work shifts, after-hours arrangements, backup and “all-hands-on-deck” arrangements (West-Brown et al., 2003). “The working hours make a huge difference in the number of staff and the needed facilities” and therefore influence funding as well (ENISA, 2006, p. 19).

ENISA (2006) and West-Brown et al. (2003) advise that the need for 24x7 operation, versus services during office hours only, should be considered. For after hours operation the following is advised:

- consider availability and equipment requirements;
- use on-call or scheduled duty rosters;
- provide limited, emergency only services; and
- “follow-the-sun” by partnering with peers in other time zones.

Smith (1994, p. 22) provides further guidelines for 24x7 operation if required.

[1] These include redundancies for leave and illness.

4.2 Roles and responsibilities

Staff roles, responsibilities and accountability need to be defined for the CSIRT and associated processes (Alberts et al., 2004, p. 27; Guttman & Roback, 1995, p. 12). The actual assignment will depend on the structure of the host organisation, the size of the constituency and the services offered (Killcrece et al., 2003a, p. 14). According to Killcrece et al. (2003b, p. 72), "many teams implement the concept of a core team [first responders and technical staff] and an extended team [temporarily added professionals or specialists] as their model for CSIRT operations". This approach is confirmed in other literature and is therefore reflected below.

4.2.1 Core team

The roles mentioned in literature (presuming that the team will be hosted in a parent organisation) are shown in table 4.1.

Table 4.1: Core staff roles for CSIRTs

	Alberts et al. (2004)	Cichonski et al. (2012)	ENISA (2006)	ENISA (2010)	Killcrece et al. (2003a)	Killcrece et al. (2003b)	Northcutt (2003)
Manager or team lead	✓	✓	✓		✓	✓	
Assistant/backup manager					✓	✓	
Technical lead		✓					
Incident lead/coordinator	✓	✓		✓			
System, platform or network administrators	✓				✓	✓	✓
Ad-hoc technical / subject area experts		✓	✓				✓
Incident handler(s)	✓	✓	✓	✓		✓	
First responders (help desk, hotline, triage)	✓			✓	✓	✓	
Vulnerability and artefact analysts	✓					✓	
Researchers			✓				

These standard, agreed upon roles for the core technical team are summarised in this section. *(Note: optional roles are marked with an *; dedicated roles are marked with a #; other roles can be shared between actors.)*

Team manager#

The team manager provides strategic direction, supervises the team and liaises with upper management and other parties (internal/external) (Alberts et al., 2004; Killcrece et al., 2003b). This role is responsible for ensuring that the necessary staff, resources and skills are provided enabling and facilitating the work of team members (Cichonski et al., 2012; Killcrece et al., 2003b).

Assistant manager*

This role acts primarily as a backup for the team manager and supports him/her by providing day-to-day operational guidance and tasks to the team (Killcrece et al., 2003b). Depending on the size of the team and the availability of the team manager this role can be considered optional.

Technical lead

The technical lead is ultimately responsible for the quality of the technical work done and should have strong technical skills and experience (Cichonski et al., 2012).

Incident lead*

This leader or project coordinator is accountable for the handling of a specific incident including the related actors and their tasks (Alberts et al., 2004; Cichonski et al., 2012). They will act as the primary point of contact for the incident and may coordinate team efforts (if required) (Cichonski et al., 2012; ENISA, 2010). This role is recommended for large and/or complex incidents and is commonly, temporarily filled by the technical lead or a senior incident handler.

System & Network administrators

Provide infrastructure support and platform expertise when required (Killcrece et al., 2003a).

Incident handler(s)#

Perform the actual response activities which include recording, tracking and handling of incidents and analysing related information (Alberts et al., 2004; Killcrece et al., 2003a, 2003b). Part of this role can include researching mitigation strategies and recovery options (Alberts et al., 2004). Incident handlers also coordinate the guidance (proactive or reactive) that will be provided to the constituency (Killcrece et al., 2003b). Other actions and tasks which are typically performed by incident handlers include:

- developing and disseminating information providing guidance or best practices for resolving or mitigating incidents (advisories, alerts, etc.) (Alberts et al., 2004; Killcrece et al., 2003b);
- containing ongoing malicious activity and repairing or recovering affected systems (as part of the response process) (Alberts et al., 2004);
- interacting with the CSIRT team, external experts and other partners as appropriate (Killcrece et al., 2003b); and
- mentoring of new CSIRT staff (Killcrece et al., 2003b).

Additionally, depending on the services offered by the CSIRT, incident handlers may optionally perform (Killcrece et al., 2003b, p. 73)

- education and training (including the development of training materials),
- technology-watch activities,
- IDS monitoring, and/or
- penetration testing.

First responder(s)

First responders include help desk, hotline and triage staff (Alberts et al., 2004; Killcrece et al., 2003a). This role answers the main CSIRT telephone (hotline), provides initial assistance, and records, sorts and prioritises (triages) incoming data (Killcrece et al., 2003b). ENISA (2010) refer to this role as the duty or triage officer who provides basic responses or answers enquiries (when acting as the hotline operator).

Smith (1994, p. 23) similarly discusses the role of "point duty" which serves to present a unified and professional front to the constituency as a single point of contact (which is needed for effective coordination (Northcutt, 2003)). Additionally, this role should be rotated amongst staff due to the high interrupt load and pressure (stress).

Vulnerability and artefact analyst(s)*

This role is only needed if the relevant services are provided by the CSIRT (i.e. vulnerability and/or artefact handling services). These analysts can perform the following tasks (Killcrece et al., 2003b, pp. 73–74):

- track, analyse and record vulnerability data (reports and artefacts);
- determine if and how these vulnerabilities affect the constituency;
- distribute vulnerability and patch, fix or workaround information (which is researched or developed); and/or
- liaise with CSIRTs, the constituency, vendors, external experts and others as required.

Researchers*

This role is only mentioned by ENISA (2006, p. 20). It is usually fulfilled by other technical staff members for example incident handlers during or outside of incident handling. For some teams having dedicated researchers may make sense depending on their mission and purpose.

ENISA (2010) remark that the *mandatory* first responder, incident handler and incident manager roles can be performed by one or two people if resources are limited. They do caution though that this "is very rare and is not recommended" (ENISA, 2010, p. 29).

4.2.2 Extended team

"These tasks do not necessarily have to be carried out by the incident handling team, but can also be undertaken by people in the hosting organisation" (ENISA, 2010, p. 30). The extended team could comprise of the roles in table 4.2. The following roles warrant clarification of need and responsibilities with reference to the CSIRT context.

Table 4.2: Extended staff roles for CSIRTs

	Alberts et al. (2004)	Cichonski et al. (2012)	ENISA (2006)	ENISA (2010)	Killcrece et al. (2003b)	Northcutt (2003)	Smith (1994)
Legal	✓		✓	✓	✓	✓	
Public relations	✓		✓	✓	✓	✓	
Technical specialists		✓	✓		✓	✓	
Administrative staff			✓	✓	✓		✓
Human resources	✓				✓	✓	
ICT services	✓				✓	✓	
Risk management / audit	✓				✓	✓	
Security groups					✓	✓	
External executives/management	✓				✓		
Finances	✓		✓				

Legal

Representatives from the legal department (counsel/consultants) are needed as the legal response is often outside of the expertise of the CSIRT technical staff and usually requires different skills or training (Alberts et al., 2004). Furthermore, the legal response process includes investigation, forensics, determination of liability, privacy issues, prosecution and interpreting of legal rulings. Legal representatives can assist in developing and reviewing agreements (e.g. NDAs, SLAs, EUAs) and other legal documents (e.g. contracts, briefs or press releases) (Alberts et al., 2004; Killcrece et al., 2003b). They can provide advice regarding compliance to laws and regulations applicable to CSIRT activities (ENISA, 2010; Killcrece et al., 2003b) and legally allowable responses (Alberts et al., 2004) or other legalities concerning incident management (ENISA, 2010). In addition, legal representatives can be called upon when a customer or constituent of the CSIRT requests legal advice (ENISA, 2010). Finally, this role can act as the contact for law enforcement, involving them as required (Alberts et al., 2004).

Public/media relations

These people represent the CSIRT to the press and handle any media inquiries (ENISA, 2010; Killcrece et al., 2003b) including the issuing of press releases (Alberts et al., 2004). This can be more broadly extended to the general public (Northcutt, 2003). They provide public relations advice and training to the team (ENISA, 2010) and assist in the development of information disclosure and crisis communication policies and procedures (ENISA, 2010; Killcrece et al., 2003b). Northcutt (2003, p. 7) advise against dealing directly with the press due to the possibility of misinterpretation and/or sensitive information leakage; they therefore advocate the role of a public affairs office.

Human resources

Human resources staff can assist with interviews, job descriptions, and even the realising of security training within the constituency (Killcrece et al., 2003b). Usually they are also involved in disciplinary action taken on employees and the development of associated policies and procedures (Alberts et al., 2004; Killcrece et al., 2003b).

Risk management

Risk management “help the CSIRT develop threat metrics and risk assessments for constituency systems” (Killcrece et al., 2003b, p. 74). They can further assist with determining the cost of incidents in terms of total impact and downtime (Alberts et al., 2004).

Existing security groups

These exchange incident-related information with the CSIRT and can help resolve computer or data theft cases (e.g. physical security group) (Killcrece et al., 2003b).

Some other extended roles were seen as minor due to reference in only one source. For completeness, these include representatives from compliance, critical infrastructure, the constituency and information security officers (Alberts et al., 2004). Killcrece et al. (2003b, p. 74) additionally provide explanations of the responsibilities of platform specialists, network/system administrators, web developers, trainers and technical writers in an extended CSIRT.

4.2.3 General responsibilities

Some responsibilities are shared between multiple roles/people and can be performed by different actors depending on the situation. These include (Alberts et al., 2004)

- receiving information from the constituency,
- communicating and sharing information with other roles (coordinated),
- receiving CSIRT process changes, and
- sending infrastructure improvement suggestions.

Roles and responsibilities are further defined in processes (Hunnebeck, 2011, p. 22).

4.3 Staff skills

"Having well-defined job descriptions that include a list of the roles and responsibilities for each of the CSIRT positions along with the necessary skills, experience, educational background and/or certifications and clearances required can be a helpful tool in identifying and hiring the right staff" (Killcrece et al., 2003b, p. 76).

In the literature, staff skills are grouped into two primary categories namely, technical (hard) skills and people (soft) skills. The most important knowledge areas are presented in the following sections.

4.3.1 Technical skills

These skills and knowledge should be distributed in the team (ENISA, 2010, p. 78). The acquisition of these skills is also dependent on practical and funding considerations (Cichonski et al., 2012, p. 16). "The credibility and proficiency of the team depend to a large extent on the technical skills and critical thinking abilities of its members" (Cichonski et al., 2012, p. 19). Some of these are considered specialised skills and the need for them will depend on the services provided by the CSIRT (e.g. malware analysis or forensics). Furthermore, having at least one person skilled in each major area of technology (e.g. operating systems and applications) is recommended.

The required skills are presented in table 4.3. These include the following:

- systems — operating systems, administration and security skills;
- networks — infrastructure and equipment, administration and security;
- security — principles, risks, threats, vulnerabilities/weaknesses and related attacks (overlapping with systems and networks);
- the Internet — technologies, protocols, applications and services; and
- encryption — technologies and cryptographic hash algorithms.

The team (as a whole) should have a comprehensive understanding of the technologies used by the constituency ensuring full coverage and maximum possible service provisioning (West-Brown et al., 2003, p. 168). This will also determine the appropriate skills required for the team. Finally, West-Brown et al. (2003, p. 169) caution that "wherever possible, individuals with a mix of skills should be hired to ensure that no single team member in the organization is indispensable."

Table 4.3: Technical skills for CSIRT staff

	Cichonski et al. (2012)	ENISA (2006)	ENISA (2010)	Northcutt (2003)	Smith (1994)	West-Brown et al. (2003)
Systems	✓	✓		✓	✓	✓
Networks	✓	✓	✓			✓
Security		✓	✓		✓	✓
Programming	✓		✓		✓	✓
Internet		✓				✓
Specialised (CSIRT service dependent)						
Malware analysis	✓		✓			
Forensics	✓		✓			
Intrusion detection	✓					
Risk assessment		✓				
Encryption						✓

4.3.2 Personal skills

As noted by ENISA (2010, p. 77), CSIRT personnel must be competent, trustworthy and able to communicate effectively with all parties because CSIRT work is largely customer-focused. West-Brown et al. (2003, p. 167) emphasize that following procedures and providing a professional interface are more critical attributes than technical expertise.

The following are the primary staff attributes advised by literature (ordered by number of references):

a. strong communication skills (oral and written),

b. analytical or critical thinking abilities,

c. teamwork,

d. ability to work under pressure (or in stressful situations),

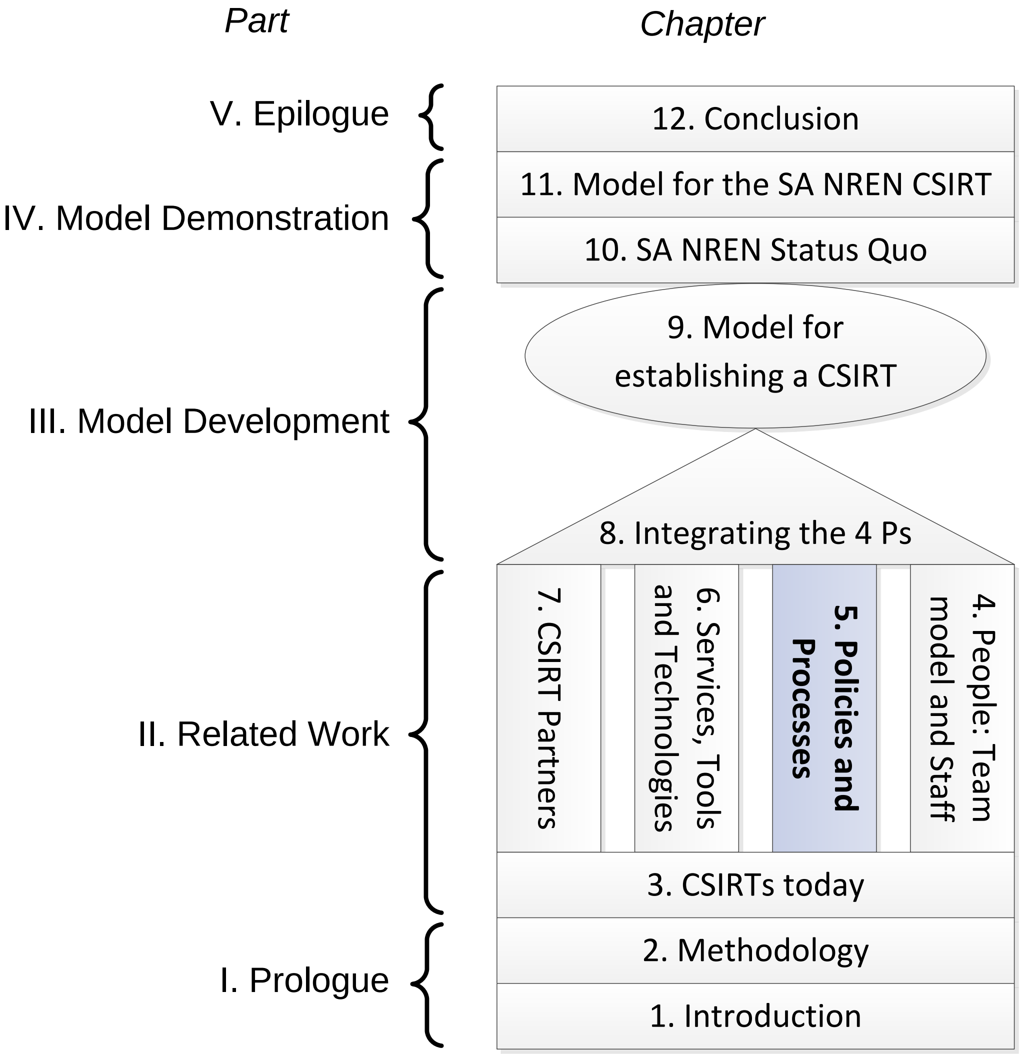
e. problem solving, and

f. aptitude for explaining technical terms to a non-technical audience.

Refer to Cichonski et al. (2012, p. 17), ENISA (2006, p. 25), ENISA (2010, p. 78), Smith (1994, p. 17) and West-Brown et al. (2003, pp. 167–168) for further elaboration on these and additional personal competencies for CSIRT staff.

4.4 Conclusion

This chapter has uncovered various *People*-related elements that need to be considered when planning a CSIRT. From the basis of the team model, the other staffing requirements follow. These include determining whether staff should be full-time or part-time, the number of staff required and work schedules. This is complemented by the definition of staff roles and responsibilities as well as the required technical and personal skills. The next chapter will look at the CSIRT *Policies and Processes* typically followed by staff when executing CSIRT services.


Part
Chapter
V. Epilogue
12. Conclusion
IV. Model Demonstration
11. Model for the SA NREN CSIRT
10. SA NREN Status Quo
III. Model Development
9. Model for establishing a CSIRT
8. Integrating the 4 Ps
II. Related Work
7. CSIRT Partners
6. Services, Tools and Technologies
5. Policies and Processes
4. People: Team model and Staff
3. CSIRTs today
I. Prologue
2. Methodology
1. Introduction

Chapter 5

Policies and Processes

According to ITIL, policies are “formally documented management expectations and intentions” (Hunnebeck, 2011, p. 411). This definition can alternatively be expressed as

> *“the governing principles under which the team operates”*
> (West-Brown et al., 2003, p. 21).

A process, on the other hand, is

> *“a structured set of activities designed to accomplish a specific objective”* (Hunnebeck, 2011, p. 412).

Alberts et al. (2004, p. C-6) similarly defines a process as “a series of actions or steps intended to bring about a desired result”. Using these definitions it can be seen that policies (governing principles) are implemented by processes (activity flows) thus providing the detailed steps needed to realise management expectations. For a team to become and remain operational, West-Brown et al. (2003, p. 3) argues that well-defined policies, procedures and services are required. Policies and operating procedures are required so that the constituency knows what services are provided by the CSIRT, whether the CSIRT will assist in a specific scenario and to aid efficient and effective interaction (Brownlee & Guttman, 1998). “When conducting interactions, one of the first issues a team should address in its policies and procedures is the level of service it is willing or able to provide to different parties” (West-Brown et al., 2003, p. 110). Service priorities, e.g. incident handling over feedback and announcements (West-Brown et al., 2003), and incident priorities, possibly using severity ratings (Cichonski et al., 2012), are also important considerations.

Killcrece et al. (2003b) found many authors agreeing that the incident response plan should be backed-up with documented policies and procedures. They argue that the CSIRT community widely embraces this concept. Furthermore, "in the absence of well-defined policies and procedures, incident handling staff (and your constituency for that matter) will make up their own rules and guidelines" which can be detrimental to the success of the CSIRT (Killcrece et al., 2003b, p. 107).

Finally, in order to facilitate the development of policies and procedures, the CSIRT objectives (mission and goals) should be clearly defined (West-Brown et al., 2003).

Following the definitions of policies and processes, this chapter is subsequently divided into two sections covering each. Section 5.1 looks at Policies from a CSIRT perspective covering generic policy contents and benefits before highlighting fundamental and secondary CSIRT-specific policies. Section 5.2 then moves to Processes, starting with the ITIL view on processes and then describing the primary CSIRT processes. These are the incident handling process and the process for generating alerts, warning and advisories. The section is concluded with a brief list of other CSIRT processes that may be required for operations.

5.1 Policies

A policy "should outline essential characteristics for a specific topic area... in such a way that all the necessary information is provided on which detailed procedures can be based to help implement the policy" (West-Brown et al., 2003, p. 39). It is a record of computer security decisions (Guttman & Roback, 1995). Policies are mainly internal guidelines dictating appropriate behaviour for specific activities (West-Brown et al., 2003).

According to West-Brown et al. (2003, pp. 39–41) policies should be

- clear and concise,
- understandable and implementable,
- necessary and sufficient,
- usable and enforceable,
- validated (translatable into real-life behaviour), and
- reviewed for legal and organisational compliance.

In this section general policy content, elements and benefits will be explored, followed by the fundamental and secondary policies applicable to CSIRTs.

5.1.1 Policy content, elements and benefits

Policy content is centred around defining behaviour in a certain topic area (West-Brown et al., 2003). Policy content guidelines provided by Cichonski et al. (2012, pp. 7–8), West-Brown et al. (2003, pp. 40–41), Guttman and Roback (1995, pp. 35–39) and ENISA (2006, p. 28) are presented in table 5.1.

Policies containing these elements are

- transparent — showing an understanding of CSIRT limitations and restrictions (West-Brown et al., 2003), and aiding efficient and effective interactions (Brownlee & Guttman, 1998);
- flexible — allowing the team to adapt to change (West-Brown et al., 2003);
- aligned and compliant — with the law, standards, etc. (ENISA, 2006; West-Brown et al., 2003);
- measurable (Cichonski et al., 2012) and quality assured (West-Brown et al., 2003);
- unambiguous (West-Brown et al., 2003); and
- considerate of resources — devoted to particular tasks and priorities (West-Brown et al., 2003).

Additionally, policies enable understanding of responsibilities and expectations (West-Brown et al., 2003) including what the CSIRT will and will not do in terms of its operation (Smith, 1994). This should include CSIRT-to-constituency and constituency-to-CSIRT response times (ENISA, 2006).

5.1.2 Fundamental CSIRT policies

The main CSIRT policies are shown in table 5.2 with references for further information. Following is a short description of each one. (Note that this excludes generic business policies such as the human resources (ENISA, 2010, pp. 77–80), legal or network policies (Alberts et al., 2004)).

Table 5.1: Generic policy elements (by author)

Policy Element	Description
Purpose and objectives	Define the issue addressed by the policy (Guttman & Roback, 1995) and consequently the purpose and objectives of the policy (Cichonski et al., 2012). Include a description of how the policy emanates from the mission statement (West-Brown et al., 2003).
Management support statement	Include a commitment from management (Cichonski et al., 2012) highlighting the organisational stand on the issue (Guttman & Roback, 1995) and endorsing this policy (West-Brown et al., 2003).
Scope and applicability	Clarify to whom the policy applies and under what circumstances (Cichonski et al., 2012) including when, where, how, to what and to whom (Guttman & Roback, 1995) the policy applies (which resources it covers).
Relationships	Relationships to services, other policies (West-Brown et al., 2003) and alignment with any applicable laws and standards (ENISA, 2006) should be described.
Glossary	To ensure that the policy is understandable to all, relevant terms and acronyms are included (West-Brown et al., 2003). Computer security incidents and related terms should be defined (Cichonski et al., 2012).
Roles and responsibilities	Roles, responsibilities and associated levels of authority must be clearly identified and defined (Cichonski et al., 2012; Guttman & Roback, 1995). This includes the people involved in the policy and their associated duties (West-Brown et al., 2003). Interaction between the parties, for example who can talk to the media and it what circumstances, should also be identified (West-Brown et al., 2003).
Processes and procedures	Essential procedures can be suggested but should not be detailed within the policy (West-Brown et al., 2003). In addition, the desired state of associated processes are described (ENISA, 2006). Accompanying (supplemental) guidelines and procedures are noted (Guttman & Roback, 1995).
Point of contact and policy maintenance	Mention who to contact for further information (Guttman & Roback, 1995). How the document is updated/maintained and who is responsible for this task should be included here (West-Brown et al., 2003). “Every policy must have a regular maintainer who keeps track of the quality of service effected through use of the policy and proposes changes to the policy as appropriate” (West-Brown et al., 2003, p. 42). This can include performance measures (Cichonski et al., 2012).

Table 5.2: Fundamental CSIRT policies

Policy	Brownlee and Guttman (1998, pp. 10–14)	Cichonski et al. (2012, pp. 7–9, 32–50)	ENISA (2006, pp. 28–29)	ENISA (2010, pp. 74–81)	Smith (1994, pp. 9–10, 16, 21–23)	West-Brown et al. (2003, pp. 141–151)
Incident reporting and request handling	✓	✓	✓		✓	✓
Data classification and prioritisation		✓		✓	✓	✓
Communications	✓	✓	✓			
Information handling and disclosure	✓	✓	✓	✓	✓	✓
Media	✓	✓		✓		✓
Privacy				✓	✓	✓
Security			✓	✓	✓	✓

Incident reporting and request handling

This is the *core* CSIRT policy. It prescribes what types of, when, to whom and how incidents should be reported (Cichonski et al., 2012; Smith, 1994; West-Brown et al., 2003). A description of what information is required, how it is recorded, as well as the expected level of service forms part of this policy (ENISA, 2006; Smith, 1994; West-Brown et al., 2003). Furthermore, it could include the tracking of CSIRT data (Killcrece et al., 2003b, pp. 88–93; West-Brown et al., 2003, pp. 91–92).

Data classification and prioritisation

This policy ensures the consistent handling of data and information (processed data (March & Smith, 1995)) by defining how it is categorised and prioritised (ENISA, 2010; West-Brown et al., 2003). Doing this helps determine when an event is considered an incident (Cichonski et al., 2012).

The categories for classifying data/information can be as simple as confidential vs public (ENISA, 2010) or "sensitive" and "other" (West-Brown et al., 2003, p. 143). West-Brown et al. (2003, p. 143) argue that these can be further divided into "fully classified", "partly classified" (shared on need-to-know basis with trusted partners) and "unclassified". Finally, the following categories are listed by (Smith, 1994, p. 16):

- Public — may be freely transmitted to anyone in plain text.
- Sensitive — information (e.g. on a vulnerability exploit) not necessarily public or widely known. Should be transmitted encrypted and shared with trusted partners or constituents on a need-to-know basis.
- Private — private constituent data only shared with that organisation's site security contact(s).
- Highly sensitive — information on sensitive sites or exploitable vulnerabilities with no solution as yet. It may be shared with trusted IRTs or constituents as needed and should always be done so encrypted (including storage).
- Classified — usually by law enforcement or the military. Requires special handling and storage according to legal requirements.

Alignment with the traffic light protocol is recommended to facilitate information handling by applying a common categorisation scheme (ENISA, 2010, p. 66). The traffic light protocol, with a suggested alignment, is described in appendix C (page 236).

Communications

Communications with external parties, including the use of secure technologies (e.g. cryptography) (Brownlee & Guttman, 1998; ENISA, 2006) and data exchange standards (Cichonski et al., 2012, pp. 48–49, 64), is defined in this policy. Key handling (West-Brown et al., 2003, pp. 108, 160–162) and notification guidelines (Northcutt, 2003, p. 3) can also be included.

Information handling and disclosure

This policy spells out what can be shared with whom (Cichonski et al., 2012; Killcrece et al., 2003b) in a consistent and secure manner (ENISA, 2010). It considers technical (Cichonski et al., 2012; Killcrece et al., 2003b), legal (ENISA, 2006) and sensitivity (West-Brown et al., 2003) aspects related to the disclosure of information.

Media

The media policy addresses how to interact with the media (ENISA, 2010; West-Brown et al., 2003) including what can be disclosed to the press, when and how (Brownlee & Guttman, 1998). This can be done together with the information handling and disclosure policy. The media policy additionally describes points of contact for the media, the CSIRT and the constituency (ENISA, 2010).

Privacy

Compliance with privacy and data protection regulations is addressed by this policy, including how private and personal data is handled (ENISA, 2010).

Security

The security policy deals with physical, personnel and ICT security (ENISA, 2006, 2010; Smith, 1994; West-Brown et al., 2003) thereby protecting the goals of other policies (West-Brown et al., 2003).

5.1.3 Secondary CSIRT policies

Other possible CSIRT policies (or policy sections) are shown in table 5.3. The applicability of these policies should be considered during the design and planning of a CSIRT and developed as required.

Table 5.3: Secondary CSIRT policies

Policy	Reference(s)
Service level agreements	Alberts et al. (2004, p. 54)
Acceptable use	Cichonski et al. (2012, p. 2), Northcutt (2003, p. 4)
Data, log and evidence retention	Cichonski et al. (2012, pp. 29, 41), Northcutt (2003, pp. 13, 34)
Code of practice/conduct	ENISA (2010, p. 81), West-Brown et al. (2003, pp. 141–142)
Human error policy	West-Brown et al. (2003, pp. 150–151)

5.2 Processes

Like emergency medical treatment, well-defined and systematic processes for responding to security-related incidents are necessary because of the pressure of incident handling and the fact that mistakes can be costly (Northcutt, 2003, p. iii). Defined procedures, together with an experienced team, help jump start the incident handling process (Killcrece et al., 2003a, p. 1). Furthermore, they can help to coordinate actions ensuring that duplicate effort is avoided and SLAs met (Alberts et al., 2004, p. 130). Processes help to minimise errors by providing standardised responses (Cichonski et al., 2012, pp. 8–9) and improving the quality of and time required to perform incident response (ENISA, 2006, p. 36).

Incident management processes should

- be *driven by the business* and integrated into other organisational processes (Alberts et al., 2004, p. 27), thus reflecting the priorities of the organisation (Cichonski et al., 2012);
- have *defined accountability* via assigned *roles and responsibilities* (Alberts et al., 2004, p. 27);
- be *supported by policies* and procedures for coordination via defined interfaces and communication channels (Alberts et al., 2004, p. 27);
- be *repeatable* (Killcrece et al., 2003b), *tested* for accuracy and usefulness (Cichonski et al., 2012) and *distributed* to all team members (Cichonski et al., 2012); and
- be *documented and reviewed* from time-to-time (Smith, 1994).

Processes implement policy statements (West-Brown et al., 2003, p. 137) and should therefore “be based on the incident response policy and plan” (Cichonski et al., 2012, p. 19). Designated staff define CSIRT policies and processes and obtain consensus and approval thereof (Alberts et al., 2004, p. 62).

5.2.1 ITIL’s view on processes and incident handling

ITIL have proposed an expanded incident lifecycle (Hunnebeck, 2011, pp. 135–137). This lifecycle, showing the stages an incident passes through, has been applied to IT security management as shown in table 5.4. “The primary benefit is that, following these phases, you can be sure that you do not omit an important part of what you have to do” (ENISA, 2010, p. 41).

5.2.2 A process for incident handling

The most important process related to CSIRTs is *incident handling.* This process provides the steps to be followed from receiving of an incident report through resolving and finally closing the incident. Although there are variations in terminology, literature studies conducted by Killcrece et al. (2003b) and referenced by Alberts et al. (2004, pp. 19–21) revealed a common process for incident handling across CSIRTs. Their list includes detection, triage, containment, analysis and response (Alberts et al., 2004, p. 3) (Killcrece et al., 2003b, p. 85).

Table 5.4: ITIL incident lifecycle applied to IT security management (based on `http://www.itsmsolutions.com/newsletters/DITYvol5iss7.htm`)

Incident phase		Description
1	Occurrence	Service disruption
2	Detection	Discovery of the event/incident
3	Diagnostics	Determining the incident root cause and characteristics
4	Repair	Reconfiguring failed/attacked systems and/or services
5	Recovery/ Restoration	Returning systems and/or services to their normal state
6	Closure	Confirmation that services are operating as normal

Combining these with a more detailed and updated process by ENISA (2010, p. 37) and with inputs from West-Brown et al. (2003, p. 77) and ENISA (2006, p. 46) results in the generic incident handling process shown in figure 5.1. The process is:

1. Report / Detect — an event is reported by a constituent, partner or other outside party and/or detected by monitoring systems (e.g. IDS).
2. Triage — the report is verified, classified, prioritised and assigned (if accepted as an incident).
3. Respond — the resolution process forms a cycle of one or more of the following:
   - analysing the report and incident;
   - determining contact information (for notification, communication and collaboration (Alberts et al., 2004));
   - containing the incident;
   - providing technical assistance;
   - researching and proposing possible resolutions;
   - executing/coordinating response actions; and/or
   - resolving, eradicating and recovering from the incident.
4. Close — an incident report is generated, all involved/affected parties are informed, incident data is archived and feedback is provided.

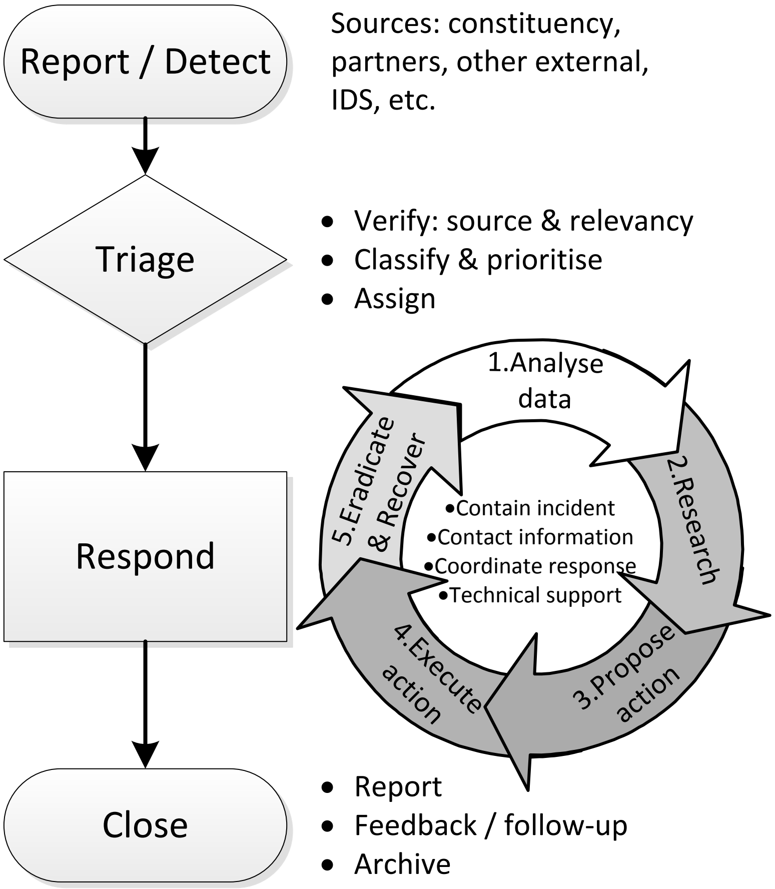


Figure 5.1: Generic incident handling process
(adapted from ENISA (2010, p. 37))

This process is mapped to the expanded ITIL incident lifecycle in figure 5.2. ENISA (2010) recommend starting with a simple model and developing the process as the CSIRT gains experience.

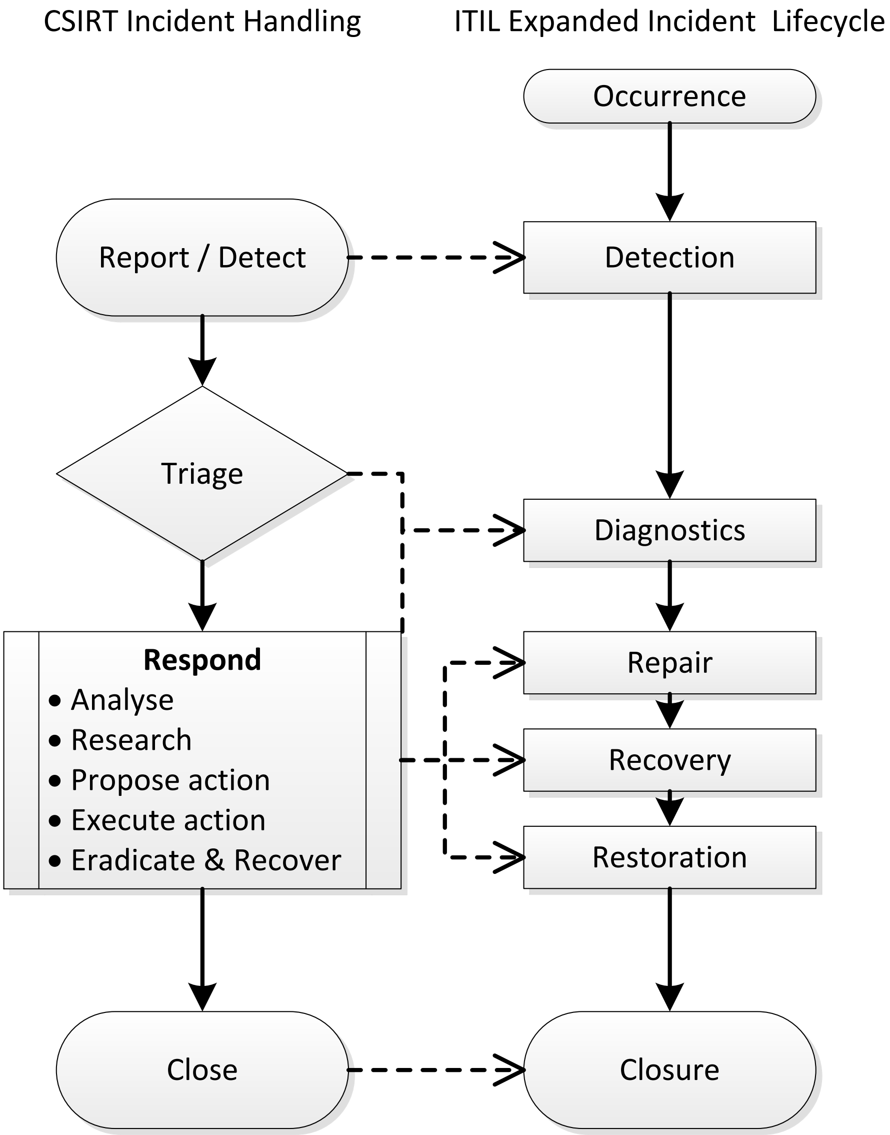


Figure 5.2: Mapping to the ITIL incident lifecycle (by author)

Responding to various types of incidents

When the team is ready for this, more information is provided on special actions for

- malicious code attacks,
- probes and network mapping,
- denial of service,
- inappropriate usage,
- espionage,
- hoaxes,
- unauthorised access, and
- intellectual property infringement (Northcutt, 2003, pp. 30–42).

Sample processes for handling unauthorised modification, network probing and completing incident recovery are provided in Appendix A of Killcrece et al. (2003b, pp. 193–195). Finally, a distributed denial of service (DDoS) response "cheat sheet" is available (ENISA, 2010)[1].

Escalation

Escalation is an important component of incident handling. It may be required to meet SLAs from the CSIRT perspective or to put more pressure on a constituent to perform resolution actions according to the AUP (Cichonski et al., 2012; West-Brown et al., 2003). It must be catered for when implementing the incident handling process in a specific CSIRT context (considering the organisation and constituency).

5.2.3 Generating alerts, warnings and announcements

The information distribution process for alerts, warnings and announcements/advisories is similar to the incident handling process and is shown in figure 5.3. This process is related to the proactive CSIRT services (see section 6.1.2, page 80) and includes "collecting information from different sources, checking it on relevance and authenticity, and redistributing it to the constituency" (ENISA, 2006, p. 36).

[1] http://zeltser.com/network-os-security/ddos-incident-cheat-sheet.pdf

The information should be verified according to origin, content and distribution channel (West-Brown et al., 2003, pp. 120–121). Relevant information is re-distributed via communication channels such as the web or email (ENISA, 2006, p. 44).

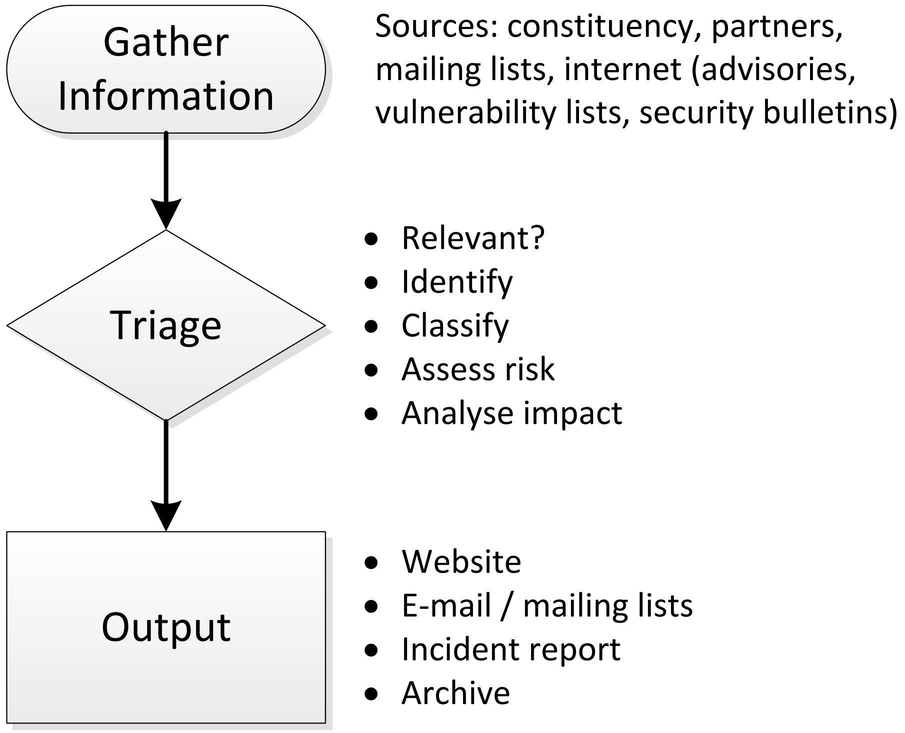


Figure 5.3: Information distribution process for alerts, warnings and announcements (based on ENISA (2006, pp. 36–44))

5.2.4 Other CSIRT processes

Some additional CSIRT processes are shown in table 5.5. Those with more than one reference are briefly described next.

Information sharing

This process complements the information disclosure policy by specifying the how, who and what of information sharing and coordination (Killcrece et al., 2003b, pp. 103–108). It overlaps in part with the previous information distribution process, particularly the "output" phase. This process can include the use of contacts lists, tools to support dissemination as well as non-disclosure agreements (Killcrece et al., 2003b, p. 104). It ensures that sensitive information is sufficiently protected and not shared with unauthorised parties (Cichonski et al., 2012, p. 9). More information related to information dissemination can be found in West-Brown et al. (2003, pp. 25, 32, 92–99).

Maintenance and tracking/recording of data

This should include what data to collect and how to access, use and archive it (Killcrece et al., 2003b, pp. 88–89). The definition of the incident reporting form and required data fields forms part of this process (Killcrece et al., 2003b, pp. 90–91). Use of a logbook for incident record keeping is additionally recommended by Northcutt (2003, p. 43). Lastly, the process includes the requirements for tools such as a tracking/ticketing system for data collection and processing. More information on tracking systems is provided in section 6.2.3 (page 85).

Public relations (media)

This process applies when dealing with the media (Alberts et al., 2004, p. 136). It should comply with the media and information disclosure policies and include the designation of a media point-of-contact, guidelines to prevent revealing sensitive information and a procedure for handling media inquiries (Cichonski et al., 2012, pp. 10–11).

Table 5.5: Additional CSIRT processes

Process	Alberts et al. (2004, pp. 16, 22)	Cichonski et al. (2012, pp. 9–11, 36)	Killcrece et al. (2003b, pp. 80–106)	Northcutt (2003, p. 43)	Smith (1994, pp. 5, 8–11, 16, 21, 26)	West-Brown et al. (2003, pp.75, 118–121)
Information sharing	✓	✓	✓		✓	✓
Maintenance and tracking of data	✓		✓	✓		
Public relations (media)	✓	✓			✓	
Human resources	✓				✓	✓
Evidence preservation and forensics		✓	✓			
Organisational	✓					
Risk and audit	✓					
Quality assurance	✓					
Configuration & maintenance of tools	✓					
Logging		✓				
Handling vulnerabilities					✓	
Internal technical					✓	
Pre-registration of contacts						✓
Key management						✓
Handling contact information						✓

Human resources

The human resources processes apply when dealing with staff issues (Alberts et al., 2004, p. 136) and could include procedures for staff arrival and exit, extension (reaching out to others for assistance) and training (West-Brown et al., 2003, pp. 171–176). These can be based on the existing processes of the host organisation (if applicable).

Evidence preservation and forensics

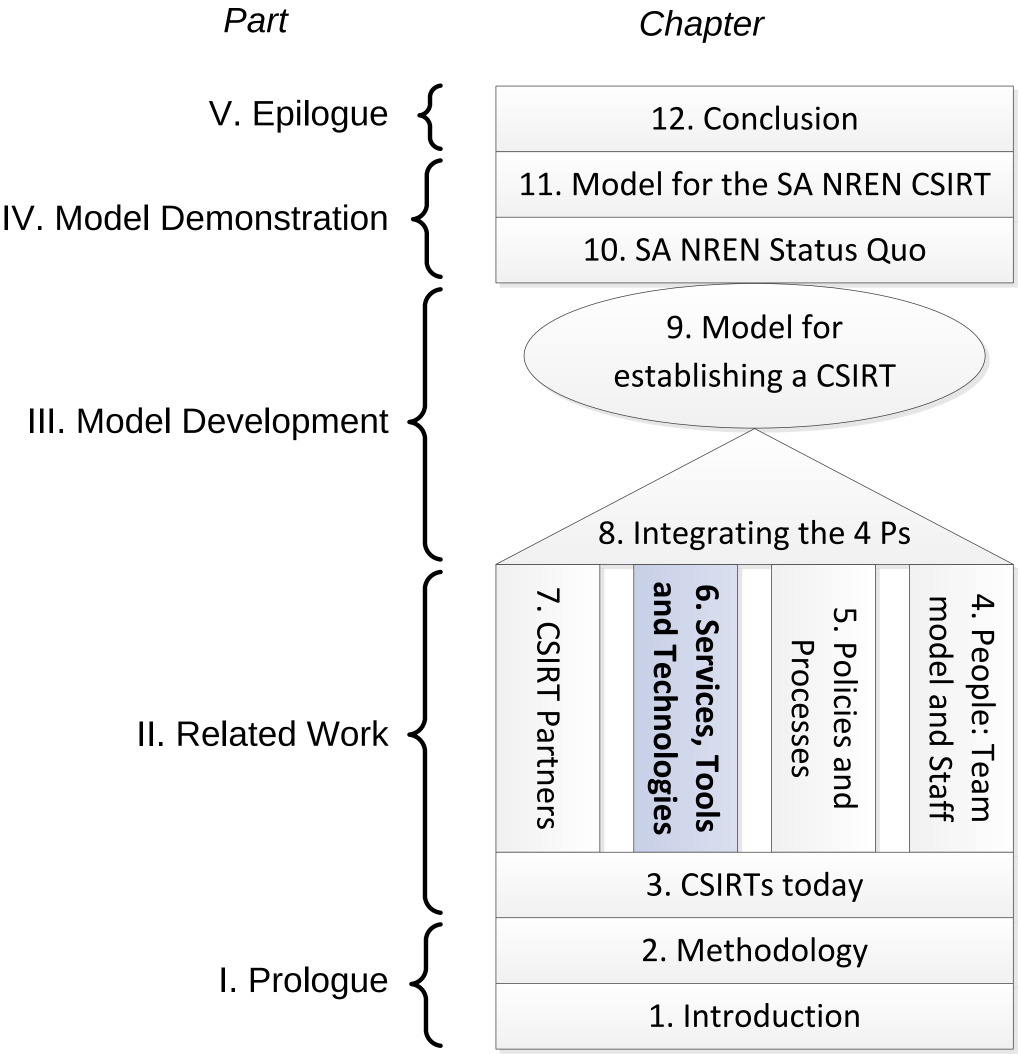
This includes procedures for forensic evidence collection and analysis that is documented, legally compliant and admissible in court (if need be) (Cichonski et al., 2012, p. 36; Killcrece et al., 2003b, pp. 98–100). Although a specialised process, users, system administrators and incident handlers "should be made aware of the steps that they should take to preserve evidence" (Cichonski et al., 2012, p. 36).

Organisational procedures include project management, IT governance and policy management (Alberts et al., 2004, p. 136). Further information on the other processes can be found in the indicated references (see table 5.5).

5.3 Conclusion

This chapter continued examining the "four Ps" requirements for establishing a CSIRT by investigating the requirements pertaining to *Policies and Processes*. Policy guidelines, descriptions of fundamental CSIRT policies and a list of secondary CSIRT policies which can also be considered, were included. CSIRT processes were looked at next, commencing with the ITIL incident handling lifecycle and combining this with CSIRT literature to define a generic process for incident handling in CSIRTs. This was followed with a process for alerts, warnings and announcements and then a brief description of other processes that may be relevant to a CSIRT.

The next chapter, chapter 6, will continue with the four Ps by looking at *Product*-related requirements: the Services provided by, and the Tools and Technologies needed for a CSIRT.


Part
Chapter
V. Epilogue
12. Conclusion
IV. Model Demonstration
11. Model for the SA NREN CSIRT
10. SA NREN Status Quo
III. Model Development
9. Model for establishing a CSIRT
8. Integrating the 4 Ps
II. Related Work
7. CSIRT Partners
6. Services, Tools and Technologies
5. Policies and Processes
4. People: Team model and Staff
3. CSIRTs today
I. Prologue
2. Methodology
1. Introduction

Chapter 6

Services, Tools & Technologies

The previous chapter looked at CSIRT policies and processes. This chapter continues with the requirements for a CSIRT by describing the services that can be provided by a CSIRT, as well as the tools and technologies supporting CSIRT work.

6.1 Services

CSIRT services were introduced in section 3.1.2 (page 35). The list of possible services is repeated in table 6.1 for convenience. Which of these services will be provided to the constituency as well as the extent of provision are important considerations when establishing a CSIRT (Killcrece et al., 2003a, p. 13).

There are three categories of services typically provided by CSIRTs, these are: reactive, proactive and security quality management services. Reactive services are the core component of CSIRT work. They are triggered by events or requests requiring a "reaction" and thereby initiating the service process (Killcrece et al., 2003a, p. 13). The execution of proactive services are intended to directly reduce the number of future IT security incidents by providing related announcements and information for preparing, protecting and securing systems (Killcrece et al., 2003a, p. 14). Security quality management services, meeting wider organisational security needs, only indirectly relate to incident handling and may be provided by the CSIRT or another entity in an organisation depending on the specific structure (Killcrece et al., 2003a, p. 14).

This section is structured according to these three categories, discussing specific services for each one in turn.

Table 6.1: CSIRT services (repeat of table 3.2)

Reactive services	Alerts and warnings Incident handling Vulnerability handling Artefact handling
Proactive services	Announcements Technology watch Security audits or assessments Configuration and maintenance of security tools, applications and infrastructure Development of security tools Intrusion detection services Security-related information dissemination
Security quality management services	Risk analysis Business continuity and disaster recovery planning Security consulting Awareness building Education and training Product evaluation or certification

6.1.1 Reactive services

"Reactive services are designed to respond to requests for assistance, reports of incidents from the CSIRT constituency, and any threats or attacks against CSIRT systems. Some services may be initiated by third-party notification or by viewing monitoring or IDS logs and alerts" (Killcrece et al., 2003a, p. 15).

Alerts and warnings

Alerts, warnings and advisories are sent as notifications of incidents, vulnerabilities or other related security matters (Killcrece et al., 2003a). They can be used to describe attacks and provide remediation or mitigation advice (West-Brown et al., 2003). Information sources for this service include the CSIRT itself, vendors, other CSIRTs, the constituency and security experts (Killcrece et al., 2003a; West-Brown et al., 2003).

Incident handling

“Incident handling includes three functions: receiving incident reports, performing incident analysis, and performing incident response. These translate into four basic services: incident analysis, incident response on-site, incident response support, and incident response coordination” (Killcrece et al., 2003b, p. 65). A team must provide at least a part of the incident handling service (i.e. incident response resolution, support and/or coordination) to be called a CSIRT (West-Brown et al., 2003). The specific sub-services offered and depth depend on the type of CSIRT (e.g. coordinating CSIRTs may rarely analyse systems) (Killcrece et al., 2003b). This service is closely linked to the incident handling process (typically following it) and includes triage, handling, announcement and feedback functions (West-Brown et al., 2003).

Vulnerability handling

This service “involves receiving information and reports about hardware and software vulnerabilities, analyzing the nature, mechanics, and effects of the vulnerabilities, and developing response strategies for detecting and repairing the vulnerabilities” (West-Brown et al., 2003, p. 28). Similar to incident handling, vulnerability handling is typically divided into three sub-services: vulnerability analysis, vulnerability response and vulnerability response coordination (Killcrece et al., 2003a). Vulnerability response coordination entails distributing vulnerability and fix/workaround information and can also include maintaining a knowledge base of vulnerabilities and corresponding response mechanisms (Killcrece et al., 2003a; West-Brown et al., 2003).

Artefact handling

An artefact in this case is “any file or object found on a system that might be involved in probing or attacking systems and networks or that is being used to defeat security measures” (Killcrece et al., 2003a, p. 19). Handling artefacts includes receiving, analysing and suggesting or developing response strategies (where applicable) (West-Brown et al., 2003).

6.1.2 Proactive services

"Proactive services are designed to improve the infrastructure and security processes of the constituency before an incident or event occurs or is detected. The main goals are to avoid incidents and to reduce their impact and scope when they do occur" (Killcrece et al., 2003a, p. 19).

Announcements

Announcements are a proactive service because they can enable the protection of systems through intrusion alerts, security advisories and warnings about vulnerabilities (West-Brown et al., 2003).

Technology watch

"This service involves reading security mailing lists, security web sites, and current news and journal articles in the fields of science, technology, politics, and government to extract information relevant to the security of the constituent systems and networks" (West-Brown et al., 2003, p. 30). Topics can include technical developments and emerging technologies, security-related trends, hacker activities and even legal, social or political issues (Killcrece et al., 2003a).

Security audits or assessments

This service performs an analysis of security infrastructure (usually for a specific organisation) based on their requirements or industry standards (Killcrece et al., 2003a). These audits can include an infrastructure review, best practice review, scanning and/or penetration testing (West-Brown et al., 2003). This service can optionally be outsourced to a Managed Security Service Provider (MSSP) or expert third party security consultant (Killcrece et al., 2003a).

Configuration and maintenance of security tools, applications and infrastructure

"This service identifies or provides appropriate guidance on how to securely configure and maintain tools, applications, and the general computing infrastructure used by the CSIRT constituency or the CSIRT itself" (Killcrece et al., 2003a, p. 21). It can range from providing guidance to performing the actual configuration and maintenance of tools, services, equipment and infrastructure (West-Brown et al., 2003).

Development of security tools

As part of this service, existing tools can be enhanced with new functionality, new tools can be developed or even patches for customised software produced (Killcrece et al., 2003a). Service activities may include building secured software distributions (West-Brown et al., 2003).

Intrusion detection services

Besides deploying intrusion detection systems, this service includes reviewing IDS logs, analysing suspicious events and forwarding alerts (West-Brown et al., 2003). To be effective, this service requires specialised tools or expertise (Killcrece et al., 2003a).

Security-related information dissemination

"This service provides constituents with a comprehensive and easy-to-find collection of useful information that aids in improving security" (West-Brown et al., 2003, p. 32). Either the CSIRT or another internal organisational unit can develop and publish the information (including processed data originating from outside partners) (Killcrece et al., 2003a). Examples of what may be included can be found in Killcrece et al. (2003a, p. 22).

6.1.3 Security quality management services

These are "well-known, established services designed to improve the overall security of an organization" (West-Brown et al., 2003, p. 32). CSIRTs can bring a unique perspective to these services due to the nature of the work and other services provided (Killcrece et al., 2003a). These services include (Killcrece et al., 2003a; West-Brown et al., 2003):

- risk analysis;
- business continuity and disaster recovery planning;
- security consulting — including advice and guidance on purchasing, installing and securing systems, network devices, applications and even policies or processes;
- awareness building — explaining security best practices/precautions;
- education and training — seminars, workshops, courses/tutorials; and
- product evaluation or certification.

These services are not necessarily provided by the CSIRT as they could be hosted by other departments depending on the structure of the organisation (Killcrece et al., 2003a, p. 13).

Most CSIRTs do not provide all of these services but rather a subset based on the type of CSIRT and the needs of the constituency (Killcrece et al., 2003a, p. 14). Furthermore, Killcrece et al. (2003a, p. 14) argue that "it is much better to perform a few services well than many services badly". A CSIRT should therefore select a core service offering and grow that as the need arises and resources allow (Killcrece et al., 2003a, p. 24). Additionally, Killcrece et al. (2003a) provide a recommended list of core services for each type of CSIRT as well as guidelines for extending service offerings.

The next section will discuss CSIRT tools and technologies as the other side of *product* considerations.

6.2 CSIRT tools and technologies

In order to distinguish the difference between tools and technologies, the Oxford dictionary provides the following definitions:

> Technology: *"The application of scientific knowledge for practical purposes."*[1]
>
> Tool: *"A device or implement... used to carry out a particular function."*[2]

Certain tools and technologies are required before CSIRT operations can commence (Smith, 1994) and for the provision of services in a secure environment (Killcrece et al., 2003a). These facilitate the resolution of computer security incidents, handling of sensitive information, and cooperation and coordination (Alberts et al., 2004; Cichonski et al., 2012).

Security technology is additionally used to address concerns such as confidentiality, integrity and availability. For example, digital signatures can be used to verify the source of information (Smith, 1994) and encryption can be used to exchange sensitive information (Killcrece et al., 2003a). Tools like firewalls and intrusion detection systems can be used to protect or alert of attempts to access CSIRT data and systems (Killcrece et al., 2003a).

[1] http://www.oxforddictionaries.com/definition/english/technology

[2] http://www.oxforddictionaries.com/definition/english/tool

Communication technologies, particularly email, should include support for data encryption and verification (ENISA, 2006; Smith, 1994). This can be achieved through the use of digital signatures, public and private keys and certificates (ENISA, 2006; Smith, 1994; Brownlee & Guttman, 1998). Communication channels should be protected against network sniffing (Smith, 1994).

The number of servers required depends on the size of the team and the services offered (Penedo, 2006). Tools are used to administer these systems and manage CSIRT networks (Alberts et al., 2004). These include anti-virus and scanning software (Killcrece et al., 2003a) as well as backup tools (Smith, 1994). Host and network security tools (e.g. firewalls, IDSs and routers with access control lists) are used to protect infrastructure components (Alberts et al., 2004; Killcrece et al., 2003a). Furthermore, security tools are used when investigating incidents (Alberts et al., 2004).

The primary CSIRT technologies and tools are presented in table 6.2. This section continues with a brief description of each category.

6.2.1 Communication mechanisms

Communication mechanisms are essential for CSIRT operations. Without them, constituents cannot report incidents and the CSIRT cannot provide assistance, consult with partners or publish advisories, etc. (ENISA, 2006). Communication approaches and channels will be determined by the communications strategy and the needs of the constituency (ENISA, 2006). Some common communication mechanisms include email, mailing lists, the web, online forms, phone, fax, hard-copy printouts, RSS feeds, video conferencing and instant messaging systems (Alberts et al., 2004; Cichonski et al., 2012; Killcrece et al., 2003a). These channels should support encryption so that it can be used where necessary or appropriate.

Some examples where encryption can be used include authentication, sensitive information distribution and identity protection (Alberts et al., 2004; Killcrece et al., 2003a). Additional guidelines for planning email and web site communications can be found in Penedo (2006). Phones should be complemented with a voice mail service and/or redirection to an after hours cell phone for 24x7 service (Cichonski et al., 2012; Smith, 1994; West-Brown et al., 2003). Backup communication methods should also be considered (Cichonski et al., 2012; ENISA, 2006). For automated reporting, email can be linked into an incident tracking/ticketing system (ENISA, 2010).

Table 6.2: Primary CSIRT tools and technologies

	Alberts et al. (2004)	Brownlee and Guttman (1998)	Cichonski et al. (2012)	ENISA (2006)	ENISA (2010)	Killcrece et al. (2003a)	Killcrece et al. (2003b)	Northcutt (2003)	Penedo (2006)	Smith (1994)	West-Brown et al. (2003)
Technologies											
Communication	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Cryptographic		✓	✓	✓		✓	✓	✓	✓	✓	✓
Tools											
Incident tracking/ticketing system (+ database)	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓
Incident handling, analysis or security tools	✓		✓	✓	✓		✓	✓	✓		✓
General hardware and software		✓	✓	✓		✓			✓	✓	✓
Network and security devices	✓		✓			✓			✓	✓	✓
System administration tools	✓				✓	✓		✓	✓		
Contacts database			✓	✓						✓	✓

6.2.2 Cryptographic mechanisms

Cryptographic mechanisms are used to address confidentiality, integrity and authenticity (Brownlee & Guttman, 1998; West-Brown et al., 2003). Depending on the classification of data, encryption can be used when communicating with external organisations (e.g. constituents, other CSIRTs and law enforcement) (Smith, 1994). The use of Pretty Good Privacy (PGP) as the standard for CSIRTs is clear (ENISA, 2006; Northcutt, 2003; Penedo, 2006). In a 2003 survey of CSIRTs, Killcrece et al. (2003b) found that 75% of participants use PGP for secure communications. Additionally, "FIRST uses PGP to protect email communications" (West-Brown et al., 2003) (as of this writing, FIRST still use PGP[3]). A PGP key can also be used to sign documents, advisories, templates, etc. as a means of verifying their authenticity (Penedo, 2006; Smith, 1994). Brownlee and Guttman (1998) recommend that every CSIRT should at least have a PGP key available and West-Brown et al. (2003, p. 160) remark that the "use of encryption and digital signature applications is unavoidable for any CSIRT". Finally, the use of cryptographic keys requires a process to manage them (Smith, 1994). The most recent RFC describing PGP is Callas, Donnerhacke, Finney, Shaw, and Thayer (2007).

6.2.3 Ticketing system and database

An incident tracking or trouble-ticketing system assigns a unique ticket to every incident (at least the triaged ones) and helps ensure timely response and resolution (Cichonski et al., 2012). This tool is used to manage incidents and track actions (ENISA, 2006). Furthermore, it facilitates cooperation between CSIRTs (Brownlee & Guttman, 1998) and can be used to link events together (Killcrece et al., 2003b). Lists of "features" that should be present in such a system are available from Cichonski et al. (2012, p. 31) and Killcrece et al. (2003b, p. 90). These include easy: searching of data, handover of incidents to other staff members and workload/distribution summaries (Killcrece et al., 2003b). Furthermore, tracking numbers are useful for announcements (West-Brown et al., 2003).

[3] see `https://www.first.org/members/application`

Examples of ticketing systems used by CSIRTs include

- Request Tracker for Incident Response (RTIR)[4] (ENISA, 2006, 2010; Killcrece et al., 2003b; Penedo, 2006),
- Open Technology Real Services (OTRS)[5] (Kácha, 2009), and
- the Application for Incident Response Teams (AIRT)[6] (ENISA, 2010; Penedo, 2006).

The most popular among CSIRTs appears to be RTIR (ENISA, 2010, p. 69)[7]. Remedy action request system, as a commercial toolkit used for building tracking systems, is another option (Penedo, 2006).

A database is typically used to complement a ticketing system for the storage and tracking of incident data (Penedo, 2006; West-Brown et al., 2003, p. 156). The database can also be used to generate statistics for reports to management and the constituency (Smith, 1994). This database is typically integrated into the ticketing system.

6.2.4 Incident handling, analysis and security tools

The are a plethora of tools that can assist in incident handling or analysis activities. These include log analysis, event monitoring, file integrity, vulnerability scanning, forensics and other investigative tools (Alberts et al., 2004; Northcutt, 2003; West-Brown et al., 2003). These either need to be obtained or developed and tested by CSIRT staff (Alberts et al., 2004). Many of these tools are related to specific services that may or may not be provided by the CSIRT.

In this category, tools are recommended for

- collecting, correlating and synthesizing incident data;
- comparing incidents with other sites and organisations; and
- determining the extent of malicious activity (Killcrece et al., 2003b).

[4] `https://www.bestpractical.com/rtir/`

[5] `http://www.otrs.com/`

[6] `http://airt.leune.com/` [note: no activity since 2009!]

[7] see also `http://www.linkedin.com/groups/RTIR-vs-OTRS-1936488.S.136507511`

To facilitate the procurement of tools for incident handling and related tasks, ENISA have compiled a "Clearing House for Incident Handling Tools" (CHIHT)[8] (ENISA, 2010, p. 67). The tools are grouped into seven functional categories, namely, tools for

1. gathering evidence,
2. investigating evidence,
3. handling evidence,
4. recovering systems (post incident),
5. implementing CSIRT operational procedures,
6. securing remote access to systems, and
7. proactive vulnerability detection and incident prevention.

The tools mentioned so far in this section are summarised in table 6.3.

Automated tools can reduce the load on human resources by performing some limited initial triage of incident reports (Cichonski et al., 2012). Some tools (e.g. event monitoring) can even be configured to automatically execute pre-planned technical responses (Alberts et al., 2004). Cichonski et al. (2012, p. 23) suggest the assembly of a "jump kit" for incident response and forensics including required software and evidence gathering accessories. More suggestions of tools for forensics are provided by Penedo (2006).

Lastly, online tools can be used to find contact information for reporting incidents such as the Réseaux IP Européens (RIPE) "whois" database[9] or trusted introducer[10] (ENISA, 2006).

6.2.5 General hardware and software

A non-exhaustive list of hardware and software that may be used by a CSIRT is provided with references in table 6.4. Networking equipment includes switches and routers (Brownlee & Guttman, 1998). Servers are required to host DNS, mail and web services as well as software tools for the CSIRT (Penedo, 2006). Laptops can be used for data analysis, packet sniffing and report writing (Cichonski et al., 2012; Killcrece et al., 2003a) and smartphones for after hours support and communications (Cichonski et al., 2012).

[8] http://www.enisa.europa.eu/act/cert/support/chiht

[9] http://www.ripe.net/data-tools/db

[10] https://www.trusted-introducer.org/

Table 6.3: Incident handling, analysis and security tools (by author)

Tools for individual systems
Log analysis
File integrity
Event monitoring
Recovery
Secure remote access
Auditing
Tools for the network
Event monitoring
Vulnerability scanning
Auditing
Monitoring
Intrusion detection
Tools for incident handling
Tracking system
Triage (automated)
Gathering information online
Tools for forensics
Gathering evidence
Investigating evidence
Handling evidence
Tools for statistics / correlation
Comparing incidents
Determining the extent of malicious activity
Correlating and synthesizing incident data

These systems should be supportable by CSIRT staff, updated and hardened before connecting them to the Internet and have redundant connectivity (where applicable) (ENISA, 2006). The choice of operating system(s) (OS) depends on the skills of the team, the cost, and the systems in use by the constituency. Linux is noted as the OS of choice for most hackers and IT security consultants (Penedo, 2006). Virtualisation can also be considered as a means to provide diverse services (Penedo, 2006). Lastly, security software includes firewall and anti-malware applications (ENISA, 2006).

Table 6.4: General CSIRT hardware and software

	Brownlee and Guttman (1998)	Cichonski et al. (2012)	ENISA (2006)	Killcrece et al. (2003a)	Penedo (2006)	Smith (1994)	West-Brown et al. (2003)
Hardware							
Networking equipment	✓						
Servers					✓		
Laptops		✓		✓			
Smartphones		✓					
Security appliances						✓	
Backup media		✓				✓	
Printer		✓					
Lab and test equipment				✓	✓	✓	
Spares (for the above)		✓					
Scanner							✓
Shredder						✓	✓
Safe						✓	
Software							
Operating systems					✓		
For secure remote access				✓		✓	✓
Security			✓				

6.2.6 Network and security devices

"Nothing makes an intruder look better than to break into a computer run by an incident response team. Nothing destroys the constituency's trust faster than if the IRT's machines are compromised" (Smith, 1994, p. 14). Security infrastructure components which can be used to hinder attackers include firewalls and intrusion detection systems:

- The *firewall* acts as a gateway to the internal network (Penedo, 2006). It should only allow selected trusted hosts to access the CSIRT subnet (Smith, 1994). A dual-screened firewall, utilising a de-militarised zone (DMZ) for publicly accessible services, will provide a high level of security; the choice and level of protection though is influenced by available budget (West-Brown et al., 2003).

- An *Intrusion Detection System* (IDS) can serve as an early warning system for IT security incidents (Northcutt, 2003). Both commercial and open source[11] varieties are available for monitoring critical network points (Northcutt, 2003, p. 3).

These are complemented by filters and access control lists on routers (Alberts et al., 2004). West-Brown et al. (2003) caution though that firewalls are essentially useless if log files are not checked regularly for suspicious events. To aid this, logging can be centralised and configured to send out alerts for unusual activity (Penedo, 2006). These, together with other defensive tools, help to identify and mitigate incidents (West-Brown et al., 2003).

For additional protection, the network and external connections should be designed and operated redundantly (using multiple providers and high-availability equipment) (West-Brown et al., 2003, pp. 162–163). Lastly, systems should be monitored, patched and updated regularly (Penedo, 2006; West-Brown et al., 2003) using system administration tools.

6.2.7 System administration tools

This is a general category including tools for configuration, patch and user management (Alberts et al., 2004) as well as host-based anti-virus and intrusion detection systems (Killcrece et al., 2003a; Northcutt, 2003). Tools for managing system backups also fit into this category (Penedo, 2006).

[11] e.g. Snort: `www.snort.org`

6.2.8 Contacts database

Contact information for the team, partners and the constituency should be stored in a contacts database or customer relationship management (CRM) system (Cichonski et al., 2012; ENISA, 2006). This facilitates access to centralised information which can be easily updated and shared across the team. Some useful contact information to obtain includes the address, telephone numbers, security contact name, email address, IP address range, and a list of hardware and software in use for each organisation (Smith, 1994). All information databases should be well protected to prevent exposure and/or manipulation of data (West-Brown et al., 2003).

6.2.9 Other CSIRT tools and technologies

Less frequently mentioned tools and technologies are presented here for completeness without further discussion. These include

- *information gathering tools* like website watchers (ENISA, 2006; West-Brown et al., 2003);
- *data sharing tools, formats and standards* such as the Incident Object Description Exchange Format (IODEF) (Alberts et al., 2004; Cichonski et al., 2012; ENISA, 2010); and
- a *knowledge base* of equipment, applications and vulnerabilities (Alberts et al., 2004; Cichonski et al., 2012).

The above should be considered for applicability when establishing a specific CSIRT.

6.2.10 Organisational tools

Finally, some tools are not CSIRT-specific and will typically form part of the infrastructure of the host organisation. These include systems or applications for

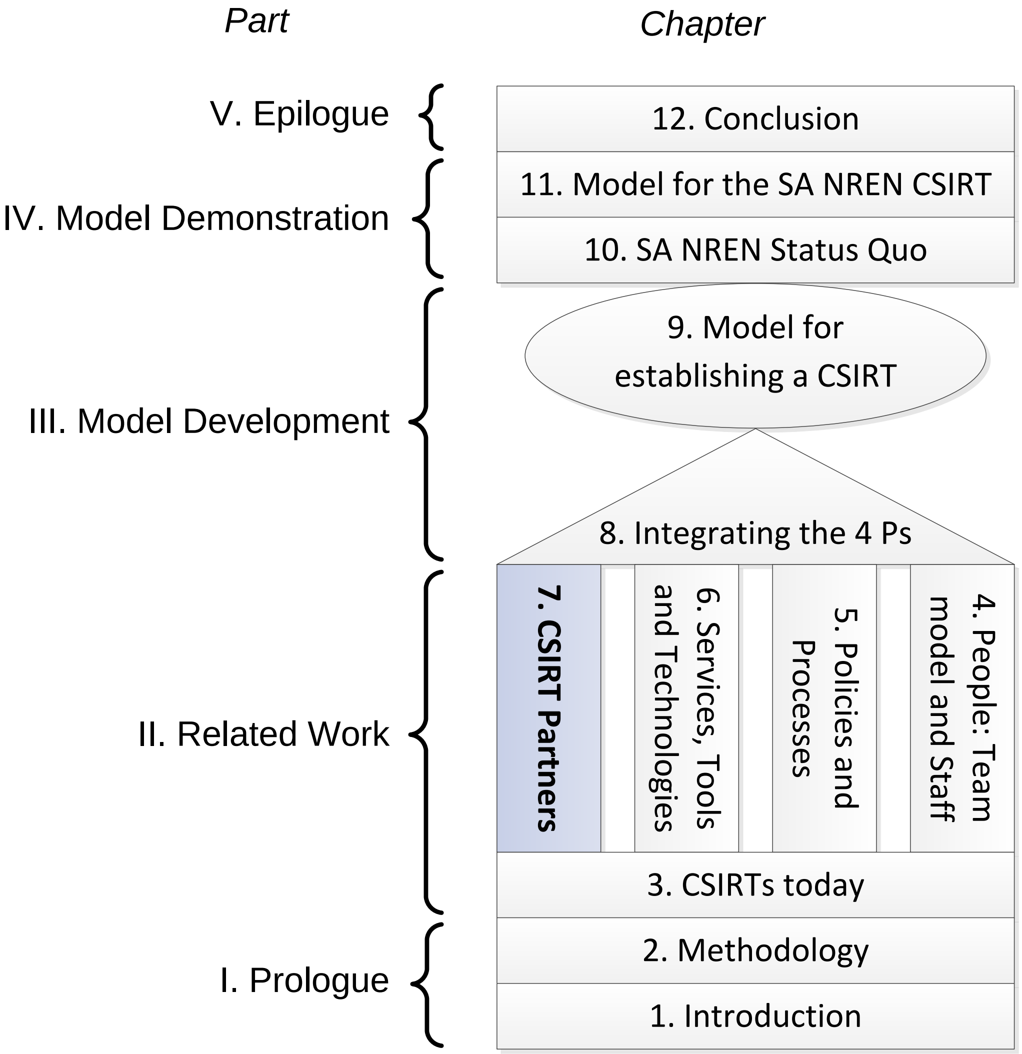
- documentation and publication,
- decision support,
- finances and accounting,
- project planning and management,
- human resources,
- purchasing,
- electronic evaluation or assessment, and
- report writing (Alberts et al., 2004).

If these tools are not provided by the host organisation, or if the CSIRT is established independently, then the CSIRT staff will need to source them as required.

6.3 Conclusion

In this chapter, CSIRT *Services, Tools and Technologies* were discussed. In the first section, the three categories of services (i.e. reactive, proactive and security quality management services) were described. The second section investigated the tools and technologies required for a CSIRT in detail. These include communication and cryptographic technologies as well as tools for tracking and handling incidents. General hardware and software, network and security devices, a contacts database and system administration tools were also discussed. The section concluded with a brief discussion of less frequently mentioned technologies and organisational tools that could be shared by the CSIRT.

The following chapter will look at the requirements related to *Partners* that are important to consider when establishing and operating a CSIRT. Both internal and external partners will be investigated.


Part
Chapter
V. Epilogue
12. Conclusion
IV. Model Demonstration
11. Model for the SA NREN CSIRT
10. SA NREN Status Quo
III. Model Development
9. Model for establishing a CSIRT
8. Integrating the 4 Ps
II. Related Work
7. CSIRT Partners
6. Services, Tools and Technologies
5. Policies and Processes
4. People: Team model and Staff
3. CSIRTs today
I. Prologue
2. Methodology
1. Introduction

Chapter 7

CSIRT Partners

Due to the nature of the Internet, incidents may occur within the constituency and affect external sites or vice versa; thus multiple sites and CSIRTs need to cooperate in resolving these incidents (Brownlee & Guttman, 1998). Furthermore, the effectiveness of the CSIRT can be improved by coordinating and sharing information with partners. Thus, enabling access to additional expertise and establishing a network of trust "to meet the needs of the incident handling process" (Cichonski et al., 2012; West-Brown et al., 2003, p. 103). The CSIRT will need to interact with various related groups while performing incident management activities and related services (Brownlee & Guttman, 1998). These groups typically include internal departments (from the host organisation) as well as other CSIRTs, law enforcement and security experts (Killcrece et al., 2003b). Killcrece et al. (2003b, pp. 104–105) found that the majority of CSIRTs share information with the CIO, the IT department, law enforcement and other CSIRTs.

This chapter briefly explores the various internal and external partners a CSIRT may need to interact with as shown in figure 7.1.

7.1 Internal partners

"It is important to identify other groups within the organization that may need to participate in incident handling so that their cooperation can be solicited before it is needed" (Cichonski et al., 2012, p. 17). These internal partners support the work of core CSIRT staff, effectively extending the team (Killcrece et al., 2003a; Alberts et al., 2004). They are shown in table 7.1 ordered by number of references.

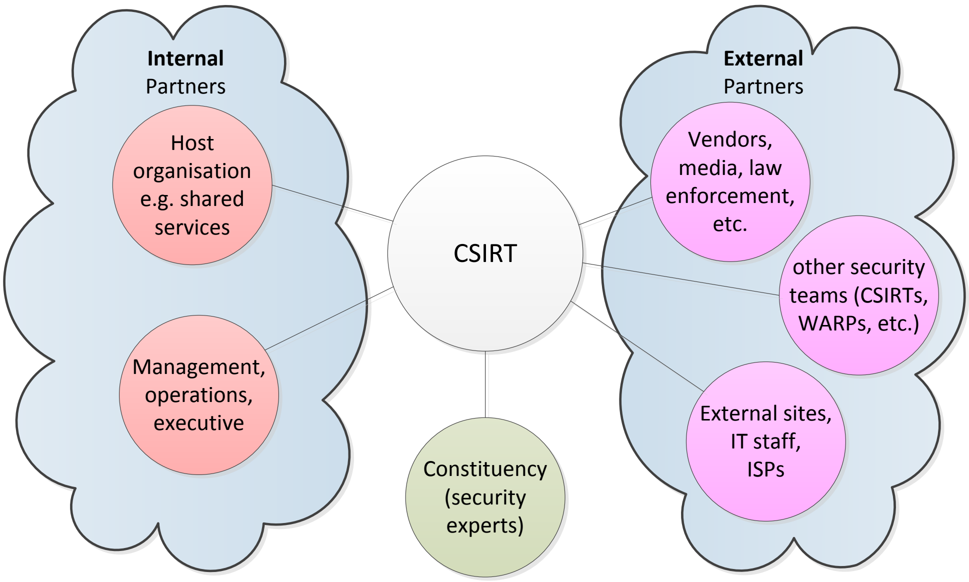

Internal Partners
Host organisation e.g. shared services
Management, operations, executive
CSIRT
Constituency (security experts)
External Partners
Vendors, media, law enforcement, etc.
other security teams (CSIRTs, WARPs, etc.)
External sites, IT staff, ISPs

Figure 7.1: CSIRT partners (based on ENISA (2006, p. 36))

Table 7.1: Internal CSIRT partners

Internal Partner(s)	Alberts et al. (2004)	Cichonski et al. (2012)	ENISA (2010)	Killcrece et al. (2003a)	Killcrece et al. (2003b)	Northcutt (2003)	West-Brown et al. (2003)
Public relations	✓	✓	✓	✓	✓		
IT administrators	✓	✓			✓	✓	✓
Legal council	✓	✓			✓		✓
Risk management	✓	✓			✓		✓
Human resources	✓	✓			✓		
Executive and management		✓					✓
Communications				✓	✓		
Facilities		✓					
Internal security teams					✓		
Help desk staff						✓	

7.1.1 Public relations

Public relations representatives are a useful interface to the media, particularly when sharing information (Alberts et al., 2004) or for incidents that may generate publicity (Cichonski et al., 2012). In addition, they can provide public relations advice and training to the team (ENISA, 2010) and assist in the development of information disclosure and crisis communication policies and procedures (ENISA, 2010; Killcrece et al., 2003b).

7.1.2 IT administrators

As knowledge experts of their domains, system and network administrators may assist in the containment or recovery of systems and related decision-making (Alberts et al., 2004; Cichonski et al., 2012). Firewall administrators and other security staff can also be used to alter firewall rules for example (Cichonski et al., 2012). These staff can trigger incident response processes through alerts from systems or examining log files (Northcutt, 2003). On the other hand, administrators have the potential to disrupt incident responses by alerting intruders or destroying evidence, due to the nature of their work (Northcutt, 2003).

7.1.3 Legal council

Legal representatives can provide expertise in investigation, prosecution, legal interpretation, forensics, liability determination as well as copyright and privacy issues (Alberts et al., 2004, p. 129). They can provide advice for compliance with relevant laws and regulations (ENISA, 2010; Killcrece et al., 2003b) or when an incident may have legal implications (Cichonski et al., 2012). Legal council can assist in developing and reviewing agreements and other documents (Alberts et al., 2004; Killcrece et al., 2003b). They can also be called upon when a customer or constituent of the CSIRT requests legal advice (ENISA, 2010). Finally, this role can act as the contact for law enforcement, involving them as required (Alberts et al., 2004).

7.1.4 Risk management

Risk management includes business continuity planning and auditing. They can help develop "threat metrics and risk assessments for constituency systems" (Killcrece et al., 2003b, p. 74) and also act in a consultancy role when incident response actions are planned, in order to minimise the disruption of business operations (Cichonski et al., 2012). Thus "incident response policies and procedures should be in sync with business continuity processes" (Cichonski et al., 2012, p. 18).

7.1.5 Human resources

Human Resources (HR) staff can assist with interviews, job descriptions and even the realising of security training within the constituency (Killcrece et al., 2003b). Additionally, HR personnel are typically involved in disciplinary action taken on employees (Alberts et al., 2004; Cichonski et al., 2012) as well as the development of associated policies and procedures (Killcrece et al., 2003b).

7.1.6 Executive and management

Internal management is ultimately responsible for the CSIRT function; they establish policies, budgets and staffing amongst other key tasks (Cichonski et al., 2012). Close relationships with management and executives is therefore essential for a successful CSIRT. This includes a relationship with the CIO/CISO, a role with security-related authority, who can escalate incidents and preventative actions (ENISA, 2010). The CIO/CISO should additionally be notified of incidents when they occur (Cichonski et al., 2012). Relationships with upper management of constituency organisations, as well as other business and functional units of the host organisation (especially the IT department), are important (Alberts et al., 2004).

7.1.7 Other internal partners

Communications partners comprise technical writers, web developers and trainers who can assist with related activities (Killcrece et al., 2003a, 2003b). *Facilities* staff provide physical security and facilities management (Cichonski et al., 2012) assisting with the physical building and accommodation related matters. *Internal security teams* span both physical and cyber security and should include existing security groups within the organisation (Killcrece et al., 2003b).

Finally, the *help desk staff* can act as the first point of contact for incident reporting (Northcutt, 2003). When using this arrangement, the help desk staff should be briefed on the kind of incidents that may be reported, as well as trained in avoiding (not being susceptible to) social engineering attacks (Northcutt, 2003).

The next section discusses the various external partners a CSIRT may need to interact with, including situational examples for these engagements.

7.2 External partners

The Internet is a global network. Security incidents can therefore span countries and even continents. One team cannot stand alone in addressing them. In order to effectively resolve these incidents, collaboration with external partners is required. External partners can also be involved when aspects of the incident (or the handling thereof) fall outside of the domain of the CSIRT. This is particularly true of criminal activity where law enforcement may be involved. In addition, the press may find out about an incident necessitating interactions with the public relations office or even the media directly.

External partners fall into two categories: trusted and general (Alberts et al., 2004). Trusted external partners may include other CSIRTs and vendors. The general category would include third-party reporters, managed security services providers (MSSPs), the media and law enforcement. A CSIRT must cooperate with these partners because reports may come from outside of the constituency; these parties may even initiate the response process (ENISA, 2010). A source from outside of the constituency may be the origin of malicious activity and because of this, partners may be needed to help resolve the incident (where possible) (ENISA, 2010). For example, an incident originating from a neighbouring country may require the assistance of the national CSIRT and/or law enforcement. Lastly, CSIRTs can team up to resolve incidents of global scale such as large virus outbreaks or distributed denial of service attacks (e.g. the 2013 Spamhaus attack).

External parties could be involved in the incident response process by either reporting incidents, being notified of security-related events, asking for help and/or being requested to provide assistance (Alberts et al., 2004). These parties are shown in table 7.2 together with the authors referring them.

Table 7.2: External CSIRT partners

External Partner(s)	Alberts et al. (2004)	Brownlee and Guttman (1998)	Cichonski et al. (2012)	ENISA (2010)	Killcrece et al. (2003a)	Killcrece et al. (2003b)	Northcutt (2003)	Smith (1994)	West-Brown et al. (2003)
Other security teams (CSIRTs)	✓	✓	✓	✓	✓	✓		✓	✓
Law enforcement	✓	✓	✓	✓	✓	✓			✓
Security experts					✓	✓		✓	✓
Vendors		✓	✓		✓				✓
Service providers (incl. ISPs)	✓		✓	✓					✓
External sites			✓	✓					✓
The press/media		✓	✓						✓
IT staff	✓						✓		✓
Coordination centres	✓		✓						
Auditors	✓								

7.2.1 Other security teams (CSIRTs)

"Relationships with other CSIRTs and security organizations can facilitate the sharing of response strategies and early alerts to potential problems" (Killcrece et al., 2003b, p. 12). Furthermore, they can provide an interface to legal agencies, law enforcement and/or external sites involved in incidents (as victims or sources) (Killcrece et al., 2003b). Joining initiatives like FIRST and Trusted Introducer (TI) can aid in soliciting cooperation with other CSIRTs (ENISA, 2006). The goals of FIRST specifically include information sharing between CSIRTs and collaborative assistance in resolving incidents via a network of coordination (Killcrece et al., 2003b). These initiatives further encourage the establishment of trust relationships between CSIRTs (West-Brown et al., 2003) and cooperation with registered vendors (Smith, 1994).

7.2.2 Law enforcement

Law enforcement can provide legal assistance and response when criminal activity is suspected (West-Brown et al., 2003). In the cases where the CSIRT wishes to report an incident to law enforcement, an understanding of applicable laws and related legal issues is essential (Killcrece et al., 2003b). Legal council can assist with this. The CSIRT in turn may advise law enforcement on the technical details of cyber attacks related to criminal activity (Brownlee & Guttman, 1998). Cooperation with law enforcement can also help to raise awareness within the community regarding prevailing incidents as well as the exchange of statistics (West-Brown et al., 2003, p. 118).

7.2.3 Security experts

Security experts include trusted members of the constituency, the parent organisation or service providers (Smith, 1994; West-Brown et al., 2003). They can be called upon to assist in areas outside of the expertise of CSIRT staff (e.g. digital forensics) or for extending staff in times of crisis (West-Brown et al., 2003)

7.2.4 Vendors

Vendors play a special role if vulnerabilities of their product(s) are involved (Brownlee & Guttman, 1998). They may analyse the problem, suggest fixes or workarounds, provide patches and test possible solutions (Brownlee & Guttman, 1998) from the perspective of understanding the threat environment (Cichonski et al., 2012). Cichonski et al. (2012) caution though that when dealing with vendors, the principle of minimum disclosure should be followed.

7.2.5 Service providers

Service providers can be called on to block major attacks or trace the origin of an incident (Cichonski et al., 2012). They can further be asked to monitor incident activity, filter network traffic or save and archive related data (e.g. log files) (ENISA, 2010).

7.2.6 External sites

External sites include affected parties, owners of attacking addresses or attack targets (Cichonski et al., 2012; ENISA, 2010). They should be notified of incidents and advised on possible remedial actions (Cichonski et al., 2012; ENISA, 2010). Real (or suspected) criminals should not be directly contacted but rather referred to law enforcement (ENISA, 2010).

Partners and their "networks" provide links to other external parties by supplying contact information or contacting Internet service/content providers directly for reporting incidents (ENISA, 2006, 2010). They may also request information (possibly for their own coordination of incident response) and provide or inquire for advice on addressing incidents (Alberts et al., 2004). These may include complaints from external sites or incidents originating from outside of the constituency (ENISA, 2010). To facilitate this, contracts or other agreements may be required (Cichonski et al., 2012; Brownlee & Guttman, 1998). Higher level CSIRTs, such as national CSIRTs, may also have requirements for reporting incident activity to them. CSIRTs can also act as a coordination point between external parties and their constituency (West-Brown et al., 2003, p. 13). Finally, partners like ISPs and law enforcement agencies can help provide or obtain information needed to resolve an incident (ENISA, 2010).

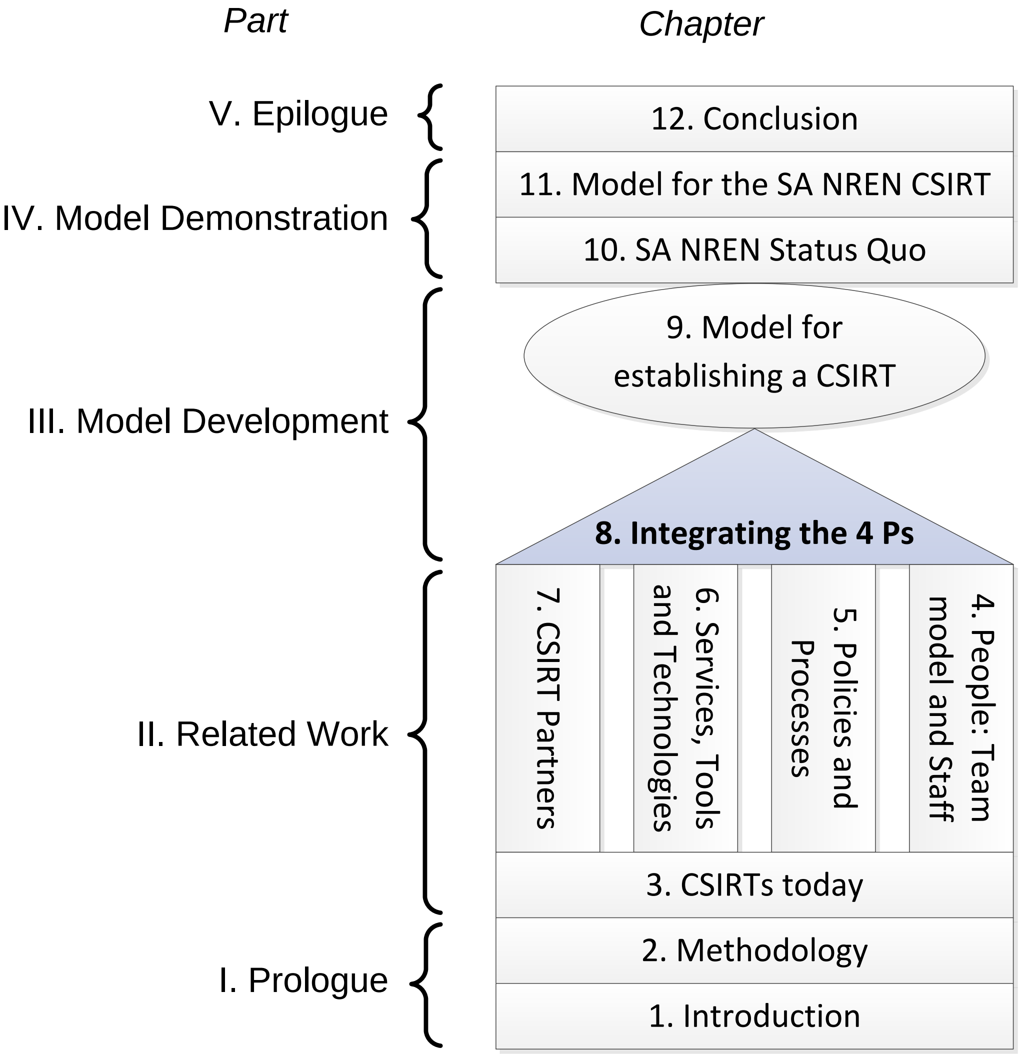
7.3 Conclusion

This chapter discussed the various internal and external *Partners* with which the CSIRT may interact. The partners in both categories were listed and their roles briefly discussed. Primary internal partners include other groups within the CSIRT host organisation such as human relations, media liaisons, IT administrators and management. Other CSIRTs and law enforcement are the main external partners that the CSIRT is likely to engage with. The remaining primary external partners were revealed to be vendors, ISPs, security experts, external sites and the press. Depending on the environment and nature of the specific CSIRTs' activities there may be varying degrees of interaction with these partners.

This chapter concludes Part II, Related Work, by completing the four Ps requirements for establishing a CSIRT as uncovered from the literature. The next chapter marks the start of the Model Development, Part III, by revealing the relationships and links between the requirements from each of the Ps. This is used as the basis for developing the generic model for establishing a CSIRT in chapter 9.

Part III

Model Development


Part
Chapter
V. Epilogue
12. Conclusion
IV. Model Demonstration
11. Model for the SA NREN CSIRT
10. SA NREN Status Quo
III. Model Development
9. Model for establishing a CSIRT
8. Integrating the 4 Ps
II. Related Work
7. CSIRT Partners
6. Services, Tools and Technologies
5. Policies and Processes
4. People: Team model and Staff
3. CSIRTs today
I. Prologue
2. Methodology
1. Introduction

Chapter 8

Integrating the Four Ps

The previous chapter marked the end of the Related Work part by revealing the various partners a CSIRT may need to work with in order to get the job done. Together with the three chapters before it, this completes the four Ps requirements for establishing a CSIRT from literature, providing the necessary background for model development.

In this chapter, the four Ps are brought together showing their relationships from a CSIRT perspective using the previous chapters as the building blocks. Although all of the primary relationships are explored, the focus is on the relationships related to establishing a CSIRT, with operational links as a secondary outcome. The connections related to establishment are therefore highlighted using bold text in the figures and additionally reflected in the section headings and summary.

The chapter commences by exploring the relationships between People and the other Ps — Processes (including Policies), Product and Partners in sections 8.1, 8.3 and 8.4 respectively. This is followed by the connections between Processes and Partners in section 8.5. Lastly, sections 8.6 and 8.7 uncover the links between Products and Processes, and Products and Partners to complete the relationships. In conclusion, a short discussion and summary of the findings is presented.

8.1 People and Processes

This section starts off the chapter by describing the relationship between the first two Ps: People and Processes. Although policies are distinct from processes, as defined in the introduction to chapter 5, they are also closely related. Policies were therefore grouped with processes as part of the same "P".

8.1.1 People develop policies & processes

Policies and processes are *developed and reviewed* from time-to-time by people (Smith, 1994). In addition, policies and processes should be *published, communicated and understood* by both the CSIRT and the constituency (Cichonski et al., 2012; Smith, 1994; West-Brown et al., 2003). This understanding ensures *appropriate actions* by staff (Smith, 1994) and *realistic expectations* from the constituency (West-Brown et al., 2003).

Staff *follow* processes (ENISA, 2010) in order to provide consistent services to the constituency (Alberts et al., 2004) aligned with *expectations* set forth in policies (ENISA, 2006). This contributes to building *trust* between the constituency and the CSIRT (Smith, 1994). Without policies and processes, people (staff and the constituency) will make up their own rules (Killcrece et al., 2003b). This clearly puts the success of the security incident response capability at risk.

8.1.2 Policies & processes formalise the team

Policies and their accompanying processes *direct* staff effort towards task completion (Guttman & Roback, 1995) and help the CSIRT *focus* on relevant requests and events during incident handling (Alberts et al., 2004; ENISA, 2006). *Boundaries* are defined by policies (West-Brown et al., 2003), and processes *specify the specific actions* undertaken (Smith, 1994) to comply with organizational and service requirements (Cichonski et al., 2012; Guttman & Roback, 1995; West-Brown et al., 2003). They describe the associated *roles, responsibility and accountability* of the various participants (Alberts et al., 2004; Cichonski et al., 2012; West-Brown et al., 2003); covering the "who" aspects of various CSIRT services (Guttman & Roback, 1995) and thereby *formalizing the team* (Killcrece et al., 2003a).

Processes facilitate pre-determined, rapid and *consistent response* to incidents (Cichonski et al., 2012; West-Brown et al., 2003) reducing the risk of incidents running out of control by delayed handling. They *guide and support* staff through the incident handling process (Alberts et al., 2004) and *reduce the risk of human error* (West-Brown et al., 2003). Finally, policies and related documentation (e.g. contracts and agreements) can facilitate *timely responses* by including CSIRT-to-constituency and constituency-to-CSIRT response times (ENISA, 2006).

The relationships described in this section are shown in figures 8.1 and 8.2.

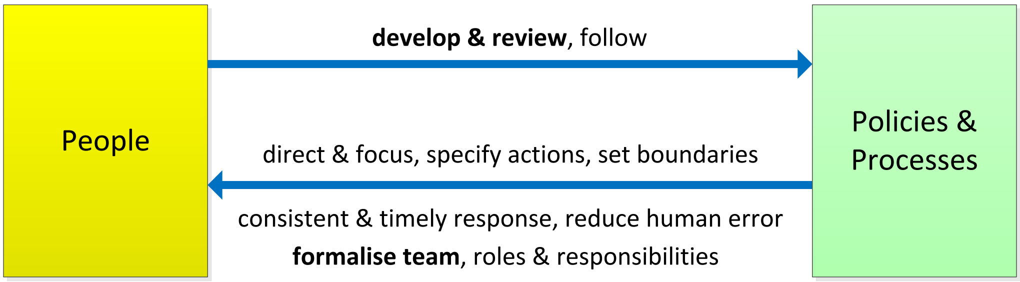

People
develop & review, follow
Policies & Processes
direct & focus, specify actions, set boundaries
consistent & timely response, reduce human error
formalise team, roles & responsibilities

Figure 8.1: Links between People and Policies & Processes

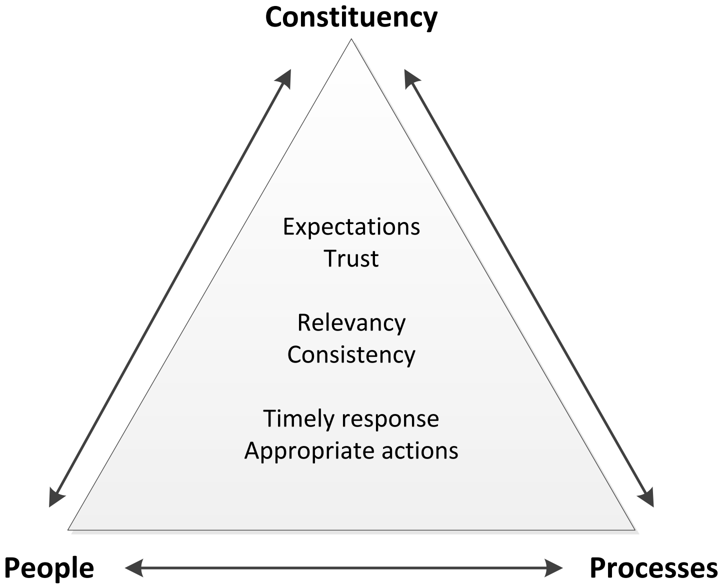


Figure 8.2: People, Processes and Constituency relationships

8.2 Product: Services, Tools & Technologies

Before moving on to the relationship between People and Product, it seemed necessary to distinguish between two categories of Product: Services, and Tools and Technologies. This section briefly describes the connections between the two categories before progressing to describe the respective relationships of each to People.

8.2.1 Services dictate required tools & technologies

While most of the services described in section 6.1 (page 77) utilise technologies in some form, some direct associations have been identified. These include the obvious *technology-related services* (e.g. technology watch, configuration and development of security tools, etc.).

The incident handling service can benefit from the use of a ticketing/ tracking system (ENISA, 2006). The triage function typically allocates a tracking number to an incident report (West-Brown et al., 2003). As previously mentioned (in section 6.2.3, page 85), this facilitates handover of incident reports to other staff (Killcrece et al., 2003b) as well as *cooperation between CSIRTs* (Brownlee & Guttman, 1998). Furthermore, tracking numbers are also useful for recording announcements (West-Brown et al., 2003). The incident handling (ticketing) system can include email/web integration for automatic *reporting* (ENISA, 2010), information collection and event correlation (West-Brown et al., 2003). This system should additionally be integrated with a database for storing incident-related data (Killcrece et al., 2003a; Penedo, 2006) and keeping track of changes (West-Brown et al., 2003). This data repository is populated by the triage function with information (optionally encrypted and/or verified) for later access (West-Brown et al., 2003). Equipment and applications provide access to, and possible hosting of, this data repository and knowledge base (Cichonski et al., 2012).

8.2.2 Tools & technologies are needed for providing services

Incident reports (as a *trigger* to the incident handling service) are received from the constituency and partners via phone, fax, email and web forms (ENISA, 2006). Similarly, these technologies are *used to provide* incident response and coordination services (Killcrece et al., 2003b). Communication technologies are *required* for security-related education and awareness services including information dissemination and answering constituency questions (Cichonski et al., 2012; Killcrece et al., 2003a). Advisories should be *distributed* using automated methods wherever possible (Cichonski et al., 2012) and mailing lists can be utilised by a technology watch service (Killcrece et al., 2003a). Test equipment and lab facilities *support* services such as artefact analysis (Killcrece et al., 2003a; West-Brown et al., 2003). Service functions can also be *triggered* by technologies (e.g. intrusion detection systems) (West-Brown et al., 2003).

These relationships are summarised in figure 8.3.

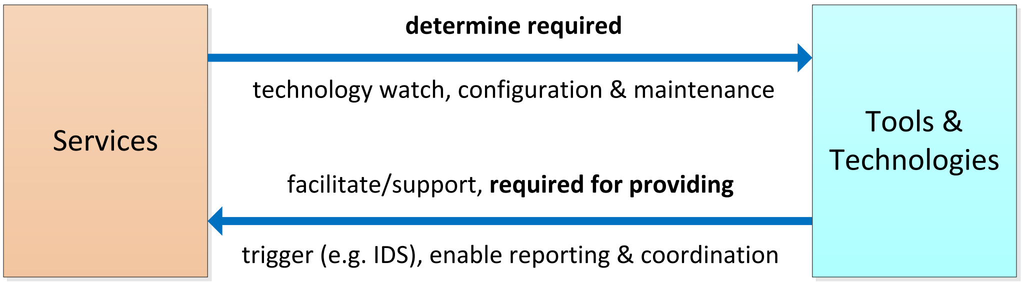

Services
determine required
technology watch, configuration & maintenance
Tools & Technologies
facilitate/support, required for providing
trigger (e.g. IDS), enable reporting & coordination

Figure 8.3: Links between Services and Tools & Technologies

The next section will investigate the links between People and Product (i.e. Services, and Tools and Technologies).

8.3 People and Product

This section explores the relationship between People and Services as well as the relationship between People, and Tools and Technologies, respectively. Both of these facilitate interactions with the constituency and partners as shown in figure 8.4 and described next.

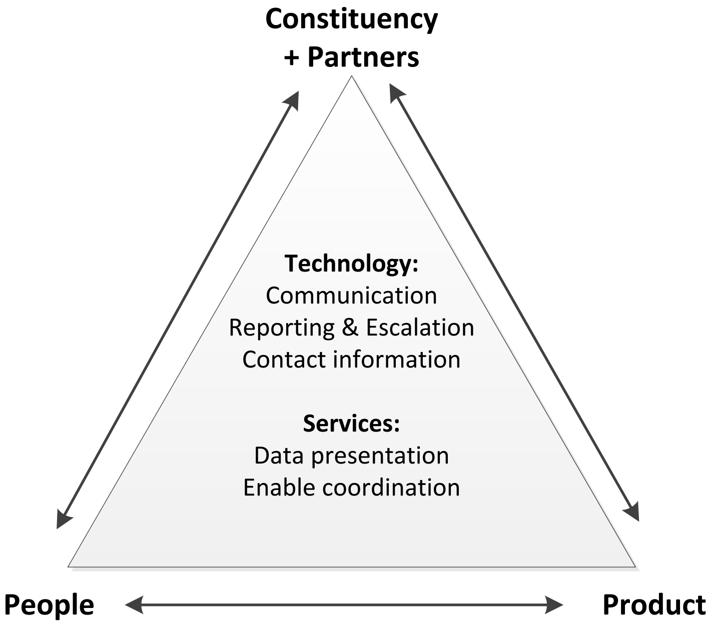


Figure 8.4: People, Product, Constituency and Partner relationships

8.3.1 People identify and develop tools & technologies

People need to *communicate*; the CSIRT needs to interact with the constituency and coordinate/cooperate with partners in order to deliver services (Killcrece et al., 2003a). Communication technologies *facilitate these interactions* (Alberts et al., 2004).

CSIRT staff *identify, organise (e.g. configure and maintain) and use* technical resources to provide security incident response services (Alberts et al., 2004; ENISA, 2006). This includes the *development and testing* of incident handling tools (Alberts et al., 2004) and the receiving of incident reports from the constituency (via phone, fax, email and/or web forms) (ENISA, 2006). Associated *contact information* is typically stored in a database for convenient, readily-available access, simplifying incident *reporting and escalation* (Cichonski et al., 2012; ENISA, 2006; Smith, 1994). Tools and technologies can also be used to *generate reports* for management (see section 6.2.3).

8.3.2 People specify services

CSIRT staff *provide* defined services to the constituency (customers of these services) (Brownlee & Guttman, 1998). How services are performed depends on who performs them (Alberts et al., 2004). The size, available expertise and skills of the team (Penedo, 2006) (i.e. human resources) influences the *quantity, type and depth* of services that can be provided. Furthermore, in addition to customers and partners, people from the CSIRT itself can *trigger* service functions (West-Brown et al., 2003).

The links between people, technology and services are shown in figure 8.5. The following sections reveal additional relationships from services, tools and technologies to people.

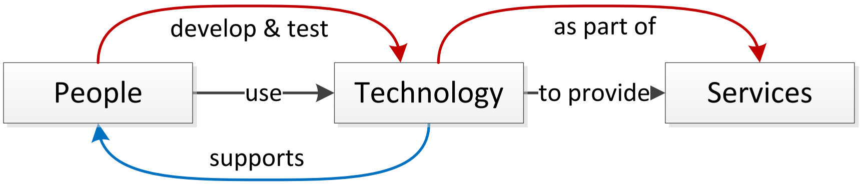


Figure 8.5: Connections between People, Technology and Services

8.3.3 Tools & technologies influence staff numbers

Tools and technologies simplify the work done by incident handlers by *automating tasks* and subsequently *reducing the staff load* (Smith, 1994) and risk of human error (West-Brown et al., 2003). These mechanisms can include the pre-processing of information (Smith, 1994) as well as selecting interesting events from logs and security software for human review (Cichonski et al., 2012). *Automated tools* can help address the vulnerability of CSIRT staff for making mistakes due to the high-stress situations and associated responsibility of the work they do (West-Brown et al., 2003, p. 150). Furthermore, tracking and ticketing systems *facilitate the handover* of incident reports to other staff (Killcrece et al., 2003b). Together with the links identified in the previous section, the relationship between People, and Tools and Technologies is depicted in figure 8.6.

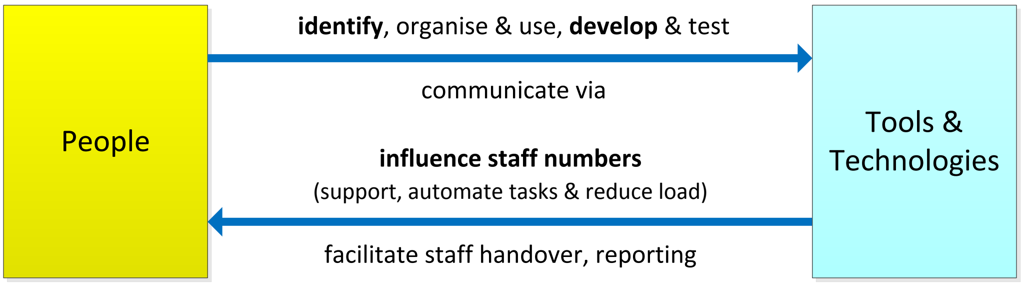

People
Tools & Technologies
identify, organise & use, develop & test
communicate via
influence staff numbers
(support, automate tasks & reduce load)
facilitate staff handover, reporting

Figure 8.6: Links between People and Tools & Technologies

8.3.4 Services define staff requirements

It has already been mentioned that people influence the quantity and type of services that can be provided. These services in turn partly determine the technical *staff requirements* (ENISA, 2006) including specialised skills (section 4.3, page 55). This is especially true of the triage function which can be executed by people internal to the CSIRT (e.g. incident handlers) or by an external help desk (Killcrece et al., 2003a, pp. 35–36). Clearly, without sufficient resources (staff and funding), services cannot be provisioned (Killcrece et al., 2003a).

Proactive services, with supporting technologies, can be used to *present* incident activity *statistics* to management (Smith, 1994). These services additionally *enable coordination* and *facilitation of interactions* between various parties (ENISA, 2006; Killcrece et al., 2003a). The relationships between services and people as uncovered in these sections are shown in figure 8.7.

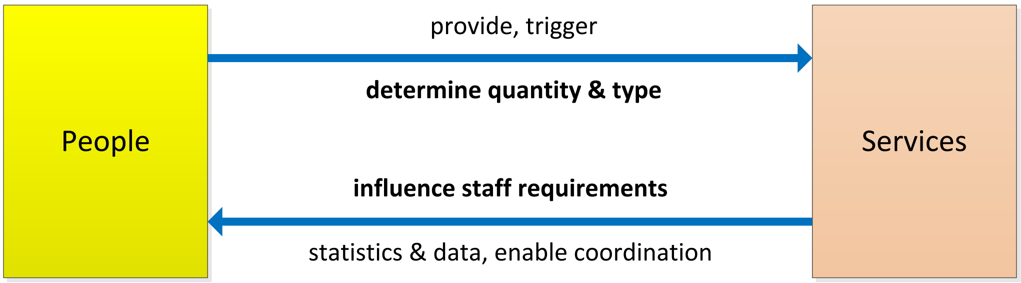

People
Services
provide, trigger
determine quantity & type
influence staff requirements
statistics & data, enable coordination

Figure 8.7: Links between People and Services

The next section explores the relationship between People and Partners.

8.4 People and Partners

From chapter 7 we see that people *identify and interact* with partners in several ways including escalating to them when applicable/appropriate (e.g. law enforcement, other CSIRTs). Partners also *assist* CSIRT staff. For example, human resources can deal with people issues; partners can also provide expertise and legal advice. They can aid with communications to/from the constituency (e.g. through a help desk as the first point of contact). This section explores these relationships in more detail.

8.4.1 People identify and coordinate partners

Trusted relationships are required with both internal and external partners (Cichonski et al., 2012) facilitating the exchange of sensitive information (Smith, 1994). These contacts and relationships should ideally be *identified and developed in advance* of when they might be required (West-Brown et al., 2003, p. 51).

CSIRT staff may be required to "*coordinate* response activities with internal departments and externally with other CSIRTs, law enforcement agencies, and security experts" (Killcrece et al., 2003b, p. 104). These partners can also assist in times of crisis (West-Brown et al., 2003, p. 51) by *relieving the workload* and/or *providing specialist skills* (Cichonski et al., 2012). Other external partners the CSIRT may be required to *collaborate* with include the media and service providers (ENISA, 2010).

The CSIRT can further act as a *coordination* point between the constituency and external parties (e.g. security or legal agencies) (Killcrece et al., 2003b; West-Brown et al., 2003). Therefore, the constituency need to understand partner *interactions*, particularly to address concerns of information disclosure (West-Brown et al., 2003). Lastly, to resolve multi-domain incidents, cooperation between sites/customers and CSIRTs is required (Brownlee & Guttman, 1998).

These connections are shown in figure 8.8.

8.4.2 Partners supplement and advise people

Other response teams can provide mutual support and technical *expertise* to the CSIRT complementing existing staff numbers and skills, and addressing deficiencies (Brownlee & Guttman, 1998; West-Brown et al., 2003).

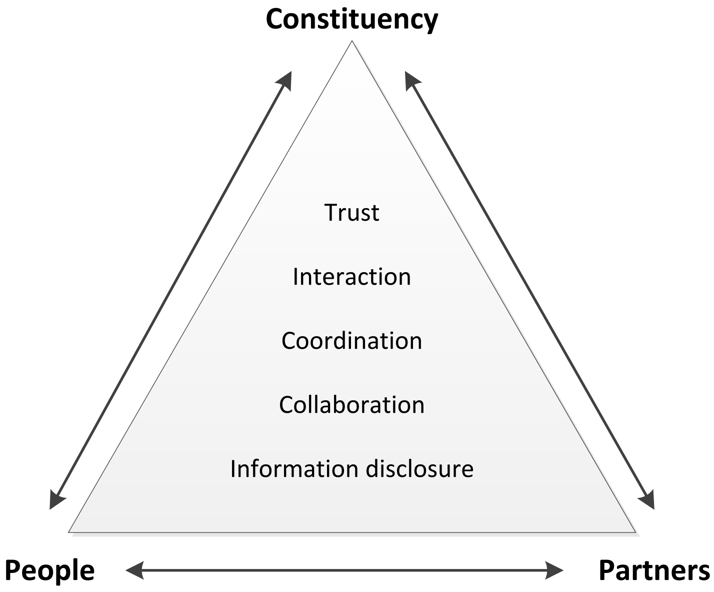


Figure 8.8: Connections between People, Partners and the Constituency

Supplementary staff can consist of people from the host organization (internal partners), the constituency, and external partners (including service providers) (Killcrece et al., 2003b; West-Brown et al., 2003). Internal partners such as technical writers, public affairs officers as well as legal and human resources consultants can *support* the work of CSIRT staff (Killcrece et al., 2003a). CSIRT management typically *coordinates* these interactions (Alberts et al., 2004). Moreover, the organizational help desk can possibly be used as the initial point of contact for incident reporting (Northcutt, 2003).

The links which have been uncovered in this section are depicted in figure 8.9.

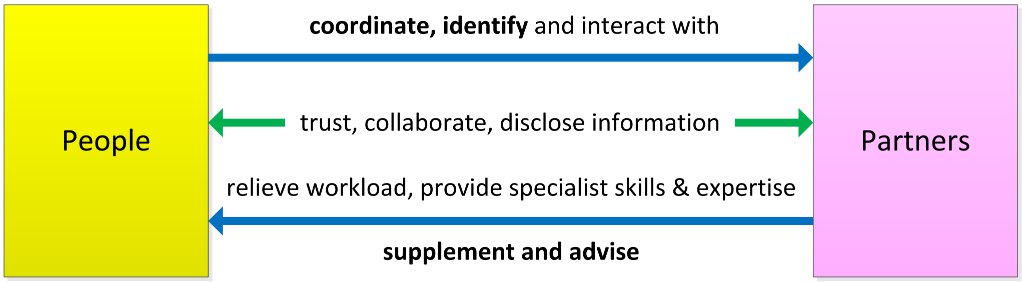

People
coordinate, identify and interact with
trust, collaborate, disclose information
relieve workload, provide specialist skills & expertise
supplement and advise
Partners

Figure 8.9: Links between People and Partners

The connections between Processes (including Policies) and Partners are revealed next.

8.5 Processes and Partners

This section describes the links from Policies and Processes to Partners and vice versa. As people develop these policies and processes, this section is brought together with the previous sections by identifying the triad of relationships between People, Processes and Partners.

8.5.1 Policies & processes define partner relationships

CSIRT preparation should include policies and procedures for *communicating* with outside parties (both internal and external partners) (Cichonski et al., 2012). Policies and procedures specify *cooperation* with external parties and include associated expected *levels of service* (West-Brown et al., 2003). Information sharing, non-disclosure and *reporting* agreements may be needed for partner *interactions* (Cichonski et al., 2012). Peering *agreements* can be established with partners (Brownlee & Guttman, 1998) who can even report events that initiate the incident response process (i.e. trigger services) (ENISA, 2006).

8.5.2 Partners help develop policies & processes

Incident handling process participants may extend beyond the CSIRT to multiple divisions and external organisations (Alberts et al., 2004). Existing teams or groups within the organisation, who may *participate in* or even *initiate* the process, should be identified and their cooperation solicited before it is required (Cichonski et al., 2012). Policies and processes typically dictate how these internal partners will work together with the CSIRT (Killcrece et al., 2003a) and can include *guidelines for* inter-departmental *cooperation* (Northcutt, 2003).

In addition, the public affairs office, legal department and management should be *consulted* by the team when establishing policies and procedures for information sharing (Cichonski et al., 2012). “Legal guidance should be incorporated into all incident response policies and procedures” (Killcrece et al., 2003b, p. 113).

Public/media relations staff *assist in the development* of information disclosure and crisis communication policies and procedures (ENISA, 2010; Killcrece et al., 2003b). In addition, human resources staff are typically involved in disciplinary action taken on employees and the *development* of associated policies and procedures (Alberts et al., 2004; Killcrece et al., 2003b).

These links revealed between policies and processes, and partners, are shown in figure 8.10.

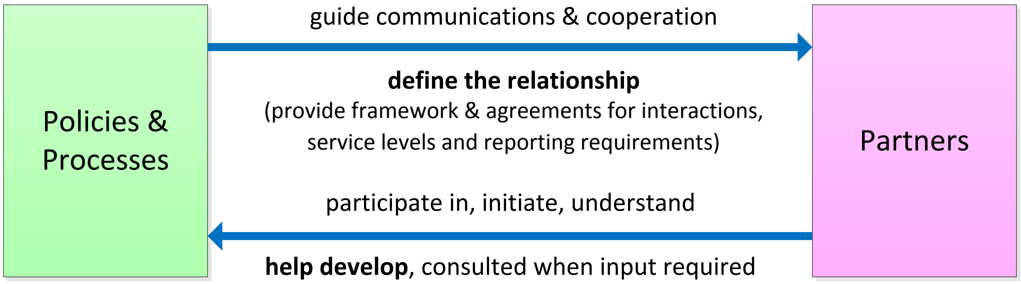

Policies & Processes
Partners
guide communications & cooperation
define the relationship
(provide framework & agreements for interactions, service levels and reporting requirements)
participate in, initiate, understand
help develop, consulted when input required

Figure 8.10: Links between Policies & Processes and Partners

Policies should be *shared with* other CSIRTs for input based on their experiences (Smith, 1994). For incident response teams to cooperate and *trust* each other, an *understanding* of each other's policies and integrity is important (Smith, 1994). This facilitates the *exchange of* sensitive *information*.

Processes can call for *coordination* to resolve incidents (ENISA, 2006) and together with policies specify how, when and at what level *interactions* with other sites, CSIRTs, law enforcement and the media occur (Killcrece et al., 2003b). For example, IT staff, dealing with the configuration, maintenance and management of systems, can be involved in the technical response process (Alberts et al., 2004, p. 97). Regarding law enforcement, policies and procedures dictate when and how incidents should be *reported* to law enforcement (Cichonski et al., 2012) as well as which and how much *information will be shared* with them (West-Brown et al., 2003).

These connections are shown in figure 8.11. The following section explores the relationship between the Processes "P" (including Policies) and the Product "P", i.e. Services, Tools and Technologies.

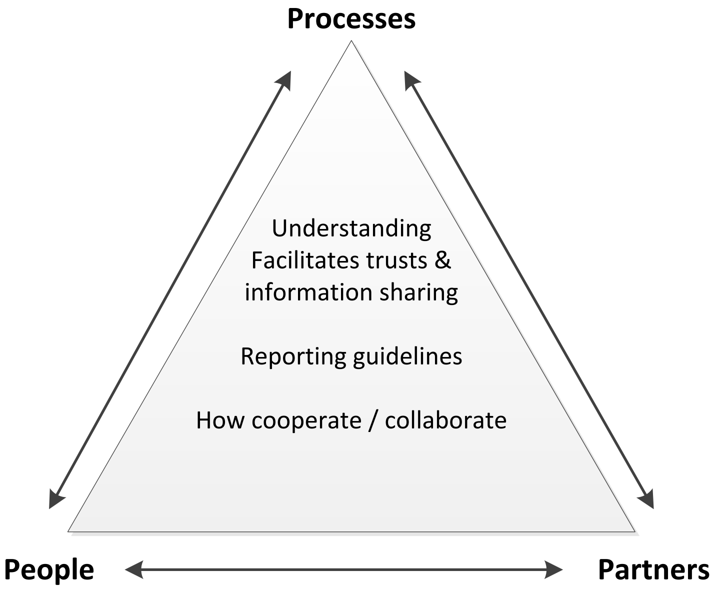


Figure 8.11: Connections between People, Partners and Processes

8.6 Processes and Product

This section uncovers the relationships between Processes (including Policies) and Services as well as Processes, and Tools and Technologies.

8.6.1 Policies & processes describe services

Policies and processes include an advertised *description* of services (Killcrece et al., 2003a). Policy dictates which services take *priority* when resources are limited (e.g. incident handling takes precedence over technology watch or awareness building) and can include process *relationships* to services (e.g. media interaction is related to incident handling) (West-Brown et al., 2003).

Additionally, successful services are *based on* appropriate policies and procedures (West-Brown et al., 2003); workflows, for instance, improve the quality and efficiency of services (ENISA, 2006). Thus processes, by their very nature, *improve service response.*

These links can be seen in figure 8.12.

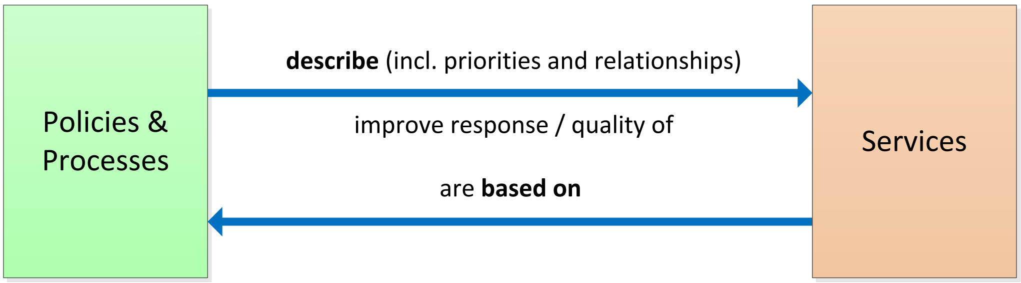

Policies & Processes
describe (incl. priorities and relationships)
improve response / quality of
are based on
Services

Figure 8.12: Links between Policies & Processes and Services

8.6.2 Tools & technologies automate processes

Policy requires visibility in order to be effective (Guttman & Roback, 1995). Technologies, particularly *communication* mechanisms, make it possible to *market and distribute* policies and processes to the constituency and other parties the CSIRT may interact with (Smith, 1994). In section 6.2 (page 82) it is further argued that tools and technologies are used to *complement* processes (for example by *automation*).

8.6.3 Policies & processes guide the development of tools & technologies

Policies and processes also support tools and technologies. This includes: *guiding the design and configuration* of automated tools (Alberts et al., 2004), system management and backup strategies (Smith, 1994), cryptographic key management (West-Brown et al., 2003) and logging systems (Cichonski et al., 2012). Moreover, security policies and best current practices should be followed by CSIRT staff when *establishing and managing* resources, equipment and infrastructure (Alberts et al., 2004).

The links from these two subsections are shown in figure 8.13.

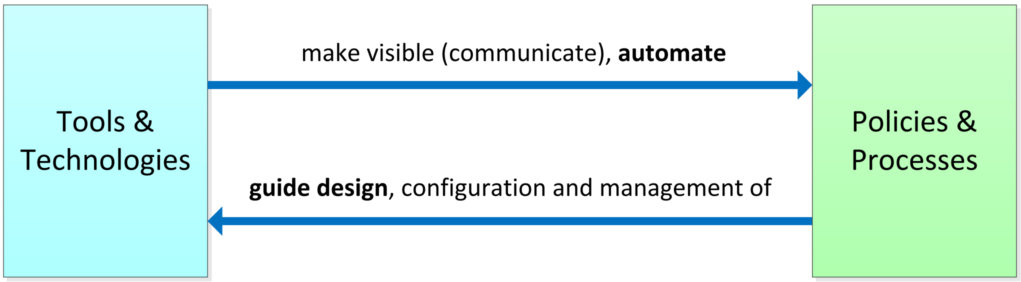

Tools & Technologies
make visible (communicate), automate
guide design, configuration and management of
Policies & Processes

Figure 8.13: Links between Policies & Processes and Tools & Technologies

8.7 Product and Partners

8.7.1 Services influence required partners

The selected CSIRT services *influence* required partnerships (West-Brown et al., 2003). Firstly, service functions can by triggered from the CSIRT itself, constituents or other parties (including partners) (West-Brown et al., 2003). Secondly, collaboration with trusted partners can *expedite* the response process, thereby *enhancing* service delivery (Cichonski et al., 2012). Lastly, incident response coordination involves the *facilitation of interactions* between involved parties (Killcrece et al., 2003a).

8.7.2 Partners provide skill and expertise to services

Partners may *participate* in (or collaborate to provide) services. To illustrate, external experts can be called upon for assistance during incident response to provide *specialised* platform or operating system *support* (Killcrece et al., 2003a). Sharing the analysis process with other *expert* groups is desirable in order to *learn* from them (gain from their knowledge and mutually enhance human capital development) (West-Brown et al., 2003).

Figure 8.14 highlights the links between Services and Partners.

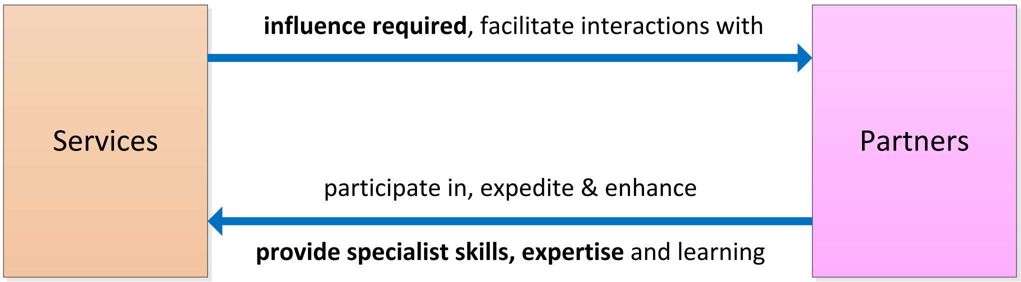

Services
Partners
influence required, facilitate interactions with
participate in, expedite & enhance
provide specialist skills, expertise and learning

Figure 8.14: Links between Services and Partners

8.7.3 Tools & technologies enable partner interactions

Technologies are used to coordinate and aid *interactions* with partners (including other teams) and outside parties (including victims) (ENISA, 2006). These include communication mechanisms (web forms, email, etc.) (Cichonski et al., 2012), data sharing tools (Alberts et al., 2004) and unique ticket numbers issued by tracking systems (Brownlee & Guttman, 1998). Cooperation and coordination is facilitated by trusted communication and information distribution channels (Alberts et al., 2004; ENISA, 2010).

Furthermore, technologies can be used to find *contact information* for external parties (ENISA, 2006). The Réseaux IP Européens (RIPE) database[1] for example, allows incidents to be routed to the correct CSIRT by providing abuse contact details. Furthermore, partner contact information is typically stored in a contacts database (Cichonski et al., 2012; ENISA, 2006).

8.7.4 Partners supplement tools & technologies

Partners can assist with *providing or recommending* CSIRT tools and technologies (via mechanisms such as the ENISA Clearinghouse for Incident Handling Tools (CHIHT)[2]). They can also be approached to assist with analysis and testing if the CSIRT does not have access to the needed equipment or technologies (Killcrece et al., 2003a) thereby *addressing* CSIRT technical *deficiencies*.

The links between Partners, and Tools and Technologies can be seen in figure 8.15.

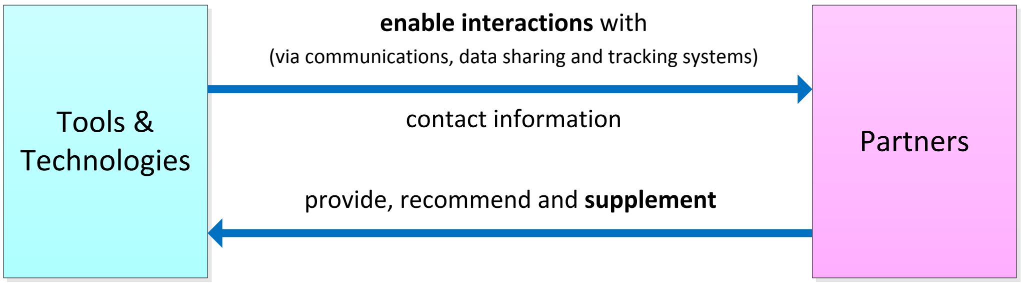

Tools & Technologies
enable interactions with
(via communications, data sharing and tracking systems)
contact information
provide, recommend and supplement
Partners

Figure 8.15: Links between Partners and Tools & Technologies

[1] http://www.ripe.net/data-tools/db

[2] https://www.enisa.europa.eu/activities/cert/support/chiht

This section marks the end of the uncovering of the relationships between the four Ps as the links from each “P” to every other “P” have been revealed. The next section will summarise the findings, showing the primary links between the Ps related to CSIRT establishment, and concluding the chapter.

8.8 Discussion

This chapter uncovered the relationships between the four Ps in detail. The relationships relevant to establishing a CSIRT can be summarised as follows (see figure 8.16):

- People *develop* Policies and Processes; Policies and Processes *formalise the team.*
- Services *determine* which Tools and Technologies are needed; Tools and Technologies are *required for* providing Services.
- People *identify and develop* Tools and Technologies; Tools and Technologies *influence staff numbers.*
- People *determine the quantity and type* of Services; Services define *staff requirements.*
- People *identify and coordinate* Partners; Partners *supplement and advise* People.
- Policies and Processes *define the relationship* with Partners; Partners provide *input to and/or help develop* Policies and Processes.
- Policies and Processes *describe* Services; Services are *based on* Policies and Processes.
- Policies and Processes *guide the development* of Tools and Technologies; Tools and Technologies are used to *communicate* Policies and Processes.
- Partners provide *skills and expertise* to Services; The selection of Services *influences the required* Partners.
- Partners *supplement* Tools and Technologies; Tools and Technologies *enable interaction* with Partners.

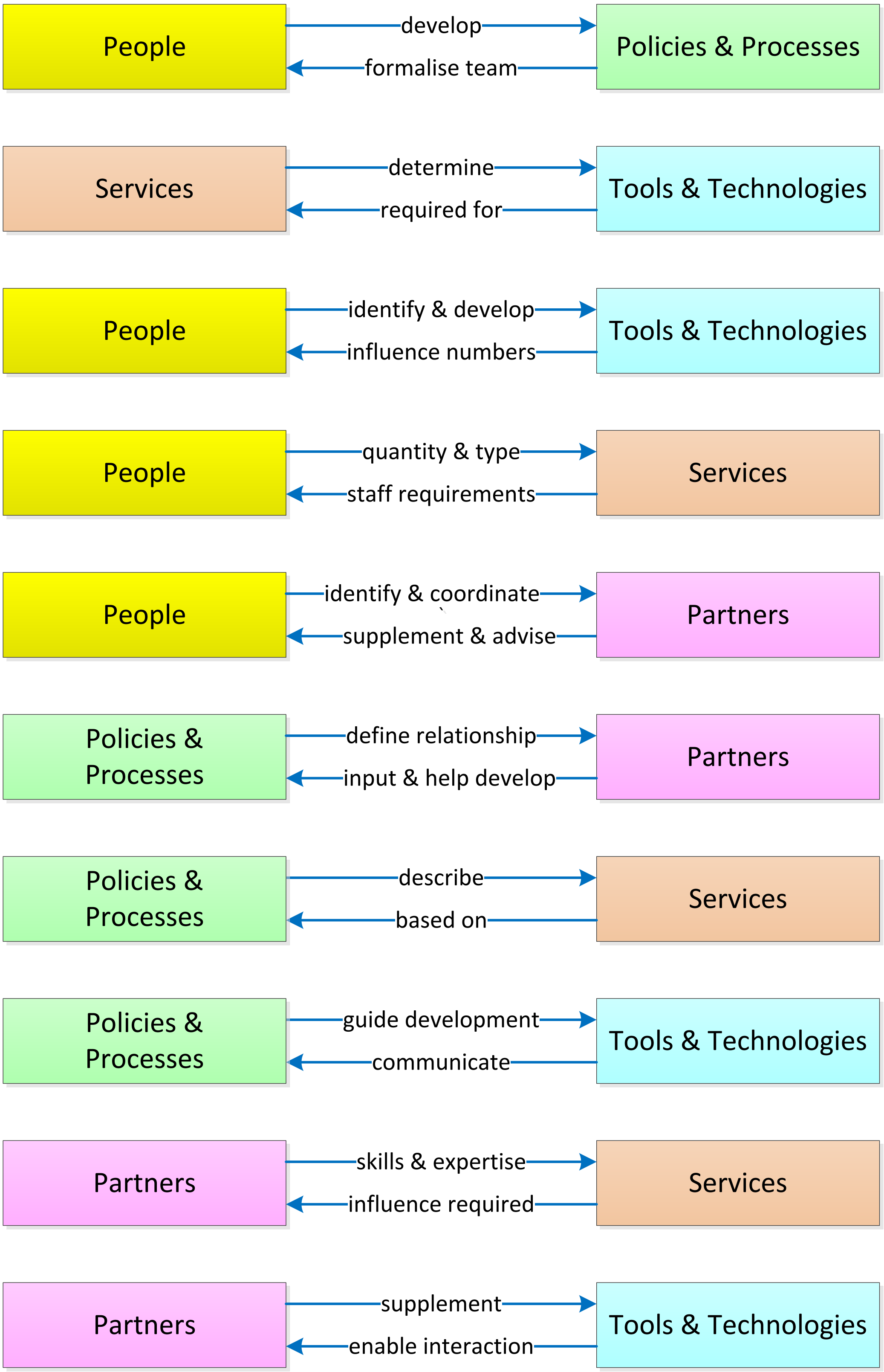
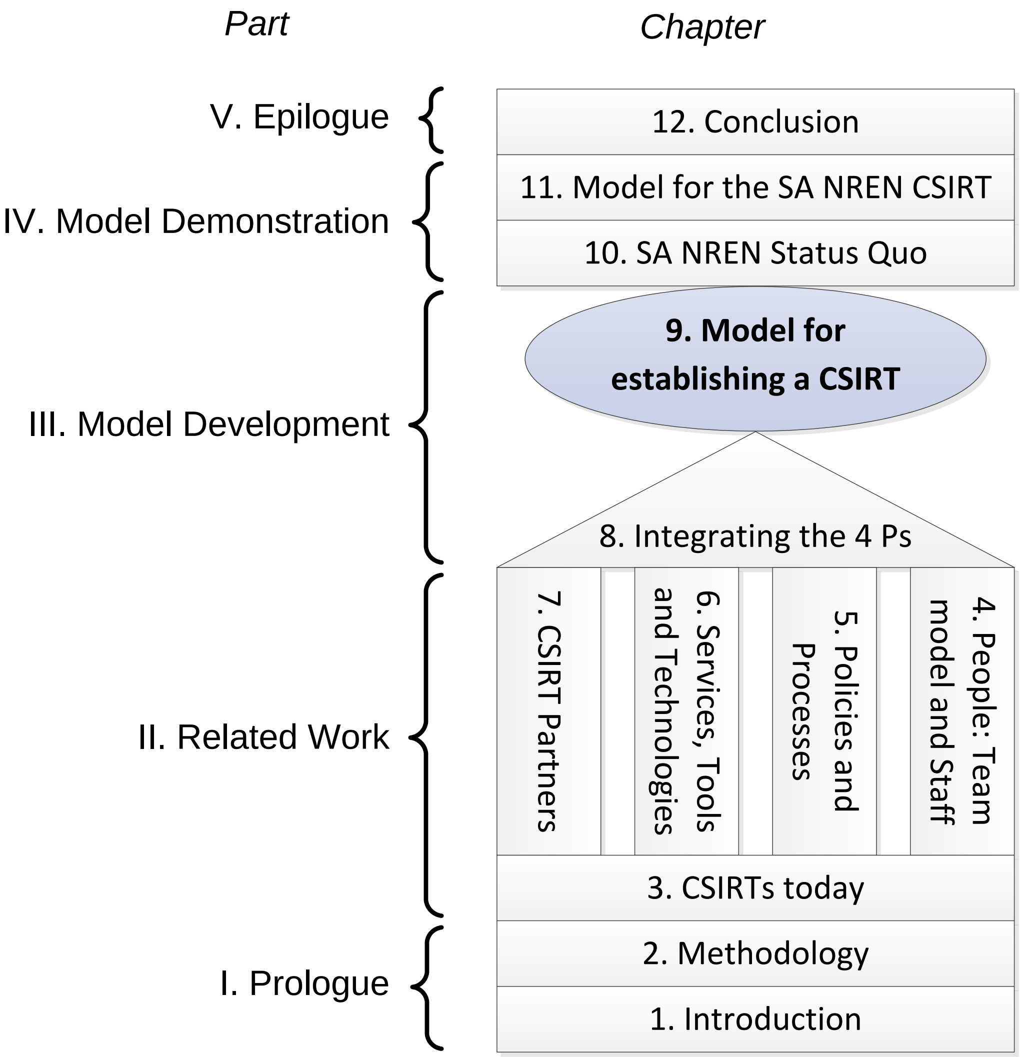


Figure 8.16: The relationships & interactions between the four Ps

8.9 Conclusion

These themes and accompanying explanations enable an holistic view when considering CSIRT requirements. They help to ensure that nothing is left out, enhancing the odds of success of the team and acceptance by the constituency. This means better incident response service delivery and ultimately a safer Internet for everyone.

The next chapter will build on the relationships by developing a generic model that can be used when establishing a CSIRT.


Part
Chapter
V. Epilogue
12. Conclusion
IV. Model Demonstration
11. Model for the SA NREN CSIRT
10. SA NREN Status Quo
III. Model Development
9. Model for establishing a CSIRT
8. Integrating the 4 Ps
II. Related Work
7. CSIRT Partners
6. Services, Tools and Technologies
5. Policies and Processes
4. People: Team model and Staff
3. CSIRTs today
I. Prologue
2. Methodology
1. Introduction

Chapter 9

Model for establishing a CSIRT

> *"To gain the greatest benefit from the use of the four Ps, organizations should determine the roles of processes and people, and then implement the tools to automate the processes, facilitating people's roles and tasks. The best way of achieving this is to develop a model or architecture based on these principles."*
> —Hunnebeck (2011, p. 61)

The basic requirements for establishing a CSIRT were explored, together with detailed requirements in four areas, namely People, Processes, Products and Partners, in the previous chapters as follows:

- Chapter 3: Business requirements. These were grouped under
  - environment,
  - constituency,
  - funding,
  - legal considerations, and
  - authority.
- Chapter 4: People: Team model and Staff.
- Chapter 5: Policies and Processes.
- Chapter 6: Services, Tools and Technologies.
- Chapter 7: CSIRT Partners.

Chapter 8 subsequently highlighted the relationships between the Ps which were uncovered during the literature review.

This chapter aims to develop a model for establishing a CSIRT based on this information. We achieve this by looking at each of the basic (business) requirements in turn, showing the relationships to other areas. This is then combined with the interactions between the four Ps, from the previous chapter, to form a big picture (i.e. holistic) model for establishing a CSIRT. An ITIL approach is used to provide the basic structure for the model as described next.

Hunnebeck (2011, p. 61) recommend that five areas need to be considered when designing a management architecture, namely

- business,
- people,
- processes,
- tools, and
- technology.

Furthermore, these areas should be designed top down and implemented bottom up as shown in figure 9.1. Considering the aim of this dissertation to develop a model for *establishing* a CSIRT, the emphasis will be on the *top-down design* process.

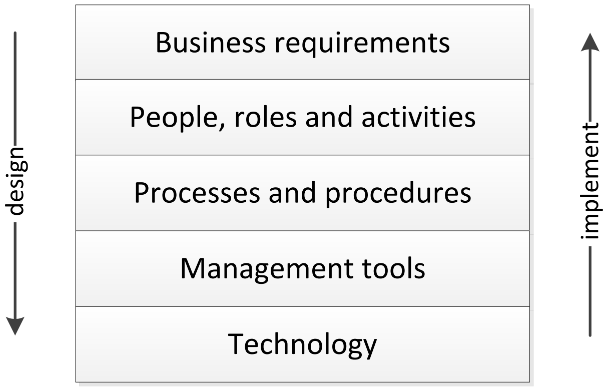


Figure 9.1: ITIL business-driven technology management (Hunnebeck, 2011, fig 3.11, p. 62)

In the context of CSIRT development, *services* and *partners* are notably missing from figure. To ensure a holistic view, these will be included on the sides of the figure as areas of “parallel development”.

In addition, tools and technologies are combined into one group to match the approach used so far in this dissertation. The amended figure is used as a framework for the rest of the model development as shown in figure 9.2.

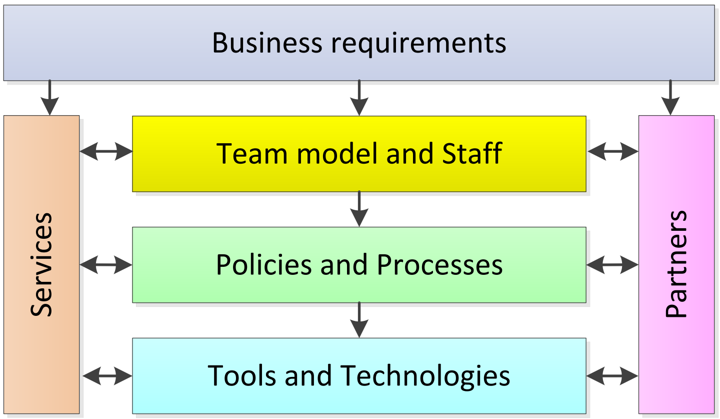


Figure 9.2: Framework for the CSIRT model (by author)
(based on figure 9.1 with the addition of partners and services on the sides)

The model should be read following this framework, paying attention to the following:

1. By executing the top-down approach, the requirements for services and partners are addressed in parallel with the team model and staff, policies and processes, and tools and technologies. This is because services and partners have interactions with all these other areas throughout the establishment exercise (as shown in chapter 8). Thus, it was decided to develop them iteratively, progressing through the sub requirements as applicable.

2. The relationship summary between any two areas is only mentioned once (in figures at least). For example, the relationship between the environment and the constituency is only mentioned in the environment section and not repeated in the constituency section. This is done to avoid duplication and preserve space. Furthermore, it has no effect on the final model, where all the links are brought together in any case.

9.1 Business requirements

The basic requirements for CSIRTs were explained in section 3.2.1 (page 36) under the headings of the environment, constituency, funding, legal considerations and authority (shown in figure 9.3). Figure 9.4 shows where these requirements fit into the framework. Each of these are discussed in turn in the following sections, highlighting the factors relevant to model development.

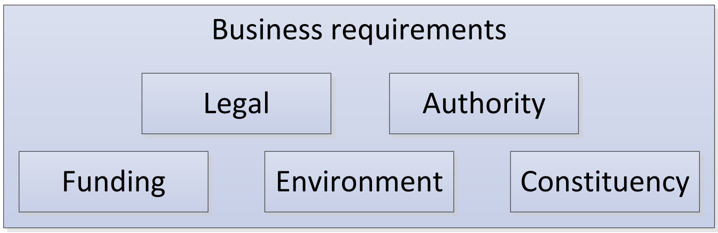


Figure 9.3: CSIRT Business requirements

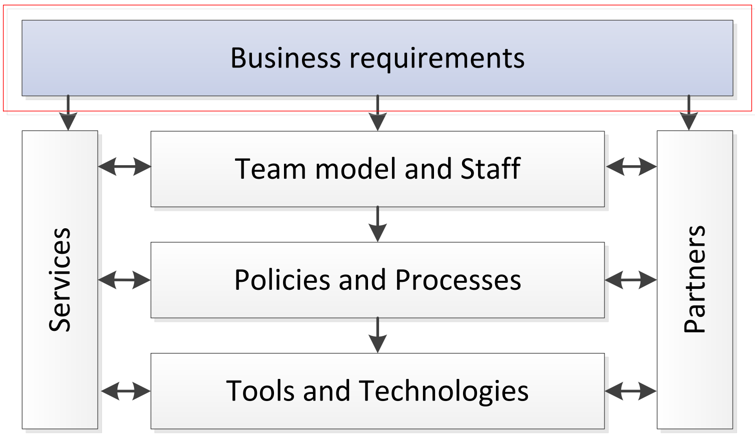


Figure 9.4: Framework showing the CSIRT Business requirements

9.1.1 Environment

To determine the environment, as argued in section 3.2.1 (page 36), the following questions need to be answered:

1. What *type* of CSIRT is it?
   (a) Is it a national, sector or individual CSIRT?
   (b) To which sector does the CSIRT belong (if applicable)? Is it an
      - academic,
      - CIP/CIIP,
      - government,
      - military,
      - SME, or
      - other (e.g. banking) CSIRT?

   (c) Alternatively, which type of individual CSIRT? Is it a
      - commercial,
      - vendor,
      - internal, or
      - other (e.g. ISP) CSIRT?

   (d) Some examples include (not prescriptive):
      - An NREN CSIRT is an academic sector (research and education) CSIRT.
      - A bank CSIRT is an internal individual CSIRT (stand alone or under a banking (other) sector CSIRT if there is one).
      - A university CSIRT is an internal individual CSIRT (usually under an academic sector CSIRT).
      - A law enforcement CSIRT could be an internal, government sector or other CSIRT depending on the specific environment.
      - The South African Cybersecurity Hub is a national CSIRT (Grobler, Vuuren, & Leenen, 2012).

2. What *geographic area* will be covered by the CSIRT?

   A global or regional CSIRT has very different implications on the constituency and services, for example, than an internal CSIRT for a single site. These include time-zones (hours of operation), languages, viable services and other issues. In addition, a CSIRT can span single or multiple cities, provinces or even countries. The geographic area has a significant influence on the team model selection.

3. Which *organisational model(s)* will the CSIRT use? Will it be

   - independent — with its own management and employees,
   - embedded — hosted in an existing organisation,
   - independently distributed among campuses, or
   - voluntary — made up of team members from the community?

Answering these questions provides a mission for the CSIRT and subsequently *reveals* the constituency. The answers also partly *determine* the team model and services provided by the CSIRT. The *mission and goals* of the CSIRT are important inputs to policies and processes (see chapter 5, page 59). The environment additionally *scopes* the legal considerations by revealing applicable laws and regulations (see section 9.1.4).

These associations are summarised in figure 9.5. Clearly, determining the environment is the first step for establishing a CSIRT.

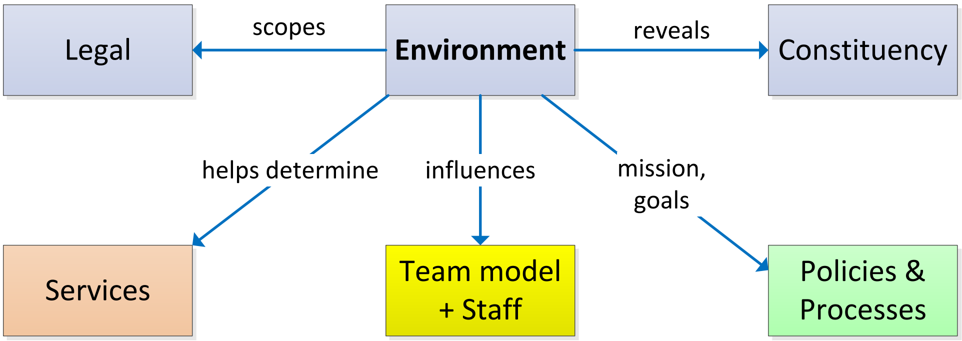


Figure 9.5: Links to/from the Environment

9.1.2 Constituency

Once the CSIRT sector and geographic region (i.e. *environment*) is identified, the constituency can be defined by one or more of the following (see section 3.2.1, page 38):

- IP address range,
- domain name,
- autonomous system number(s), and/or
- free text.

The relationships between the constituency and the four Ps are shown in figure 9.6.

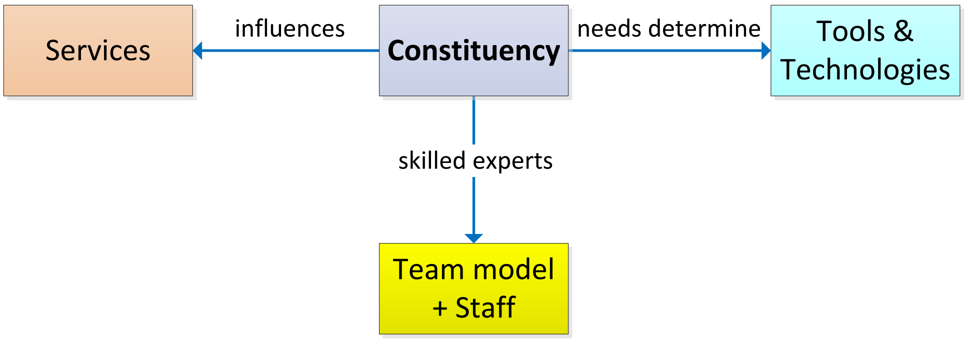


Figure 9.6: Constituency relationships

Together with the environment, the constituency *influences* the services that will be provided by the CSIRT. The team model additionally depends on the accessibility of *skilled experts* from the constituency, and/or partners, who can extend the team (see section 4.1, page 45 and section 4.2.2, page 51).

Section 6.2 revealed some important links between the constituency, and tools and technologies. Specifically, that the required communication mechanisms are *determined by the needs* of the constituency (page 83).

Other links to the constituency are not related to the establishment process and are therefore not discussed here.

9.1.3 Funding

As part of establishing a CSIRT, the *source(s) of funds* need to be identified (ENISA, 2006, p. 19). Section 3.2.1 (page 39) provided four main options: existing resources, paid membership, project subsidy and/or paid for services. Clearly, income relies on the environment as well as the nature of the constituency (e.g. whether they would be willing to pay for CSIRT services).

In section 3.2.1 it was argued that the main contributors to CSIRT expenses are the *hours of operation* and *staff salaries*. Conversely, the available budget determines *how many people* can be employed (and at which *skill* level). Thus, the team model and staffing decision go hand-in-hand with funding, determining the primary costs. The other area influenced by funding is the *equipment* required by the CSIRT.

The primary relationships involved in determining the budget and contributing to the corresponding income and expenditure are shown in figure 9.7.

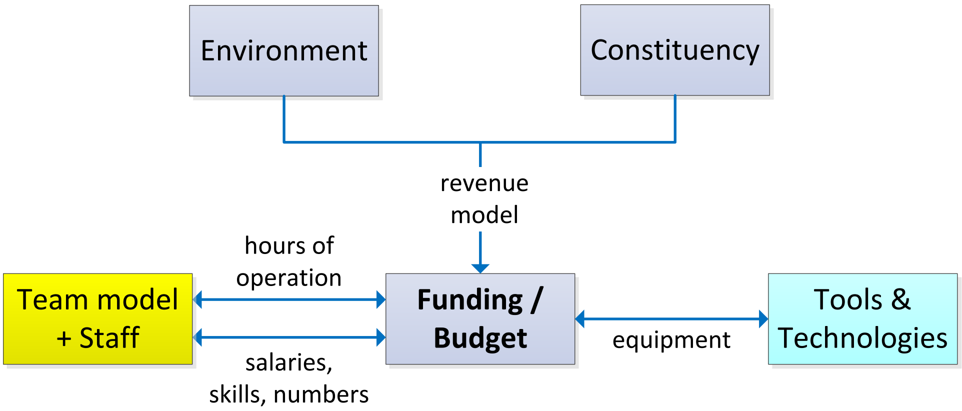


Figure 9.7: Links to/from Funding/Budget

9.1.4 Legal considerations

As noted in section 3.2.1, relevant laws are dependent on the CSIRT environment. A global CSIRT requires a different understanding of laws and regulations as compared to a CSIRT operating in a single country. (Although at least an awareness of the most important laws affecting external partners is required.) This relationship to the environment is shown in figure 9.5.

When establishing a CSIRT, legal advice should be sought on the relevant laws detailed in section 3.2.1 (page 40). Legal council and law enforcement partners can *advise on compliance* to these laws or regulations (see section 7.1.3, page 96 and section 7.2.2, page 100). The link between partners and legal considerations is shown in figure 9.8.

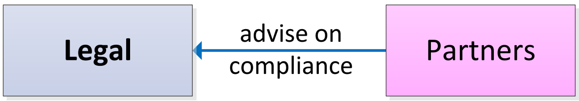


Figure 9.8: Partners advise on Legal compliance

9.1.5 Authority

The nature of the constituency *determines* the type of authority which the CSIRT may exercise over the constituency. Figure 9.9 shows this link. Once the type of authority — full, shared, indirect or none (section 3.2.1, page 40) — has been determined, it needs to be communicated back to the constituency. Previously, in the same section, it was also argued that CSIRT management staff must support the authority relationship.

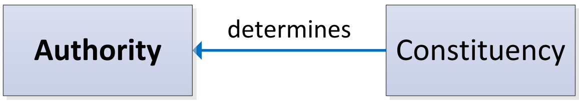


Figure 9.9: Link from the Constituency to Authority

9.2 Services

In section 3.1 (page 32) it was noted that service definitions are dependent on the constituency as well as financial and human *resources*. Clearly, before services can be defined, an understanding of *needs and expectations* of the constituency as well as the budget are required. These dependencies are portrayed in figure 9.10.

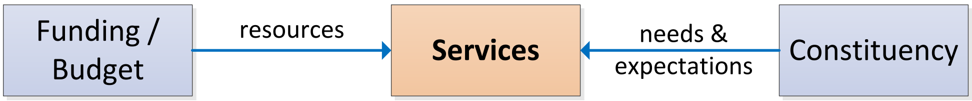


Figure 9.10: Links to/from Services

"In a perfect world the funding would be adapted to the needs of the constituency, but in reality the portfolio of services that can be provided must adapt to a given budget. So it's more realistic to start with the planning of monetary issues" (ENISA, 2006, p. 18).

Following these, the CSIRT services to be provided can be selected from table 3.2 (page 35) remembering that at least one of the incident handling services are required to be considered a CSIRT. Section 6.1 (page 77) provides more detail on the available options. To facilitate the selection of services, Killcrece et al. (2003a) provide detailed mapping of services to the various CSIRT team models. Lastly, the services portfolio can obviously be expanded as required, thereby growing with the CSIRT (Killcrece et al., 2003a, pp. 26–30).

9.3 Four Ps requirements for establishing a CSIRT

Chapter 8 showed the interactions between people, processes, product and partners from a CSIRT perspective. From that chapter, we can see two groups of relationships: firstly, requirements for establishing a CSIRT and secondly, relations when operating a CSIRT. Considering that the aim of this dissertation is to develop a model for *establishing* a CSIRT, we will focus on the first group of requirements.

Throughout chapter 8, the establishment requirements were highlighted using bold text in the figures. These requirements are summarised in figure 8.16 (page 122). This section looks at each of the four Ps in turn, briefly discussing what is required for each when establishing a CSIRT, and combining the earlier associations to build the model.

9.3.1 People: Team model and Staff

People-related aspects of establishing a CSIRT were discussed in chapter 4. The two main areas for consideration are the team model and staff. The introduction to chapter 4 (page 44) argued that the primary inputs to these areas are the environment and funding (as shown in figures 9.5 and 9.7). In addition, we have seen that access to skilled experts from the constituency can affect required staffing (section 9.1.2).

In this section, the people-related aspects of establishing a CSIRT are summarised. The relationships from chapter 8 related to people will then be discussed. Where this fits into the selected framework is shown in figure 9.11 (recalling that service and partner requirements are partly considered in parallel with the team model and staff due to the links revealed at the end of this section).

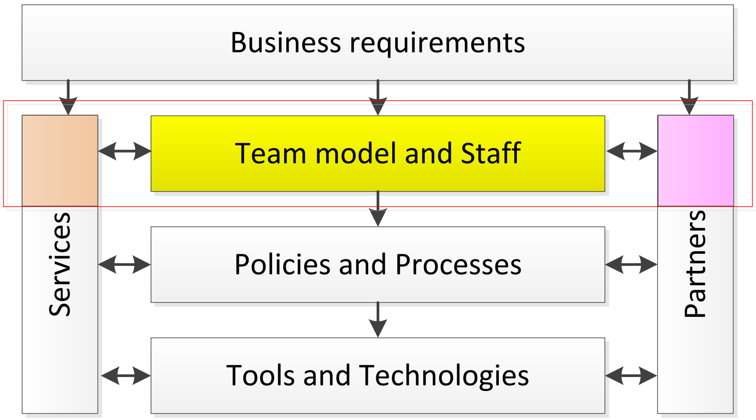


Figure 9.11: Framework for development: People

Team model

Following the specification of the environment and constituency, the team model can be determined according to section 4.1 (page 45) as

- central — in one location, fully staffed with a single point of contact;
- distributed — a “virtual” CSIRT with distributed staff (existing and/or part-time);
- coordinating — providing advice across a variety of organisations; or
- combined — best for large, distributed organisations or constituencies.

Whether *full- and/or part-time* staff will be suitable is the next decision to be made. This is closely related to the *work schedule* (hours of operation). Both of these are based on the environment, funding and need for services (from the constituency/partners). The staffing alternatives presented in section 4.1.1 (page 46) can also be considered.

As argued in section 4.1.2 (page 46), determining required *staff numbers* is not trivial. The nature of the constituency, funding and available external expertise all play a role. Until the CSIRT becomes operational, the workload, a direct determinant of required human resources, remains unknown. The best that can be done during the establishment stage is to estimate the required staffing and have a mechanism (and budget) to adapt as necessary. The ENISA guidelines (page 47) can be utilised for this purpose. Finally, section 8.4 (page 113) argues that access to partners (internal and external) as well as experts from the constituency can be used to supplement staff numbers if required.

Roles, responsibilities and staff skills

The assignment of roles, responsibility and accountability depend on the organisational structure, constituency and selected CSIRT services (as per section 4.2, page 48). These assignments can be reflected using a RACI matrix (Hunnebeck, 2011, pp. 64–68).

The core and extended teams should be defined using the information in section 4.2.

Lastly, the technical and personal staff skills described in section 4.3 (page 55) should form part of the job descriptions when hiring CSIRT staff, recalling that the need for specialised skills will depend on the selected services and the technologies in use by the constituency (section 4.3.1).

People relationships to the other Ps

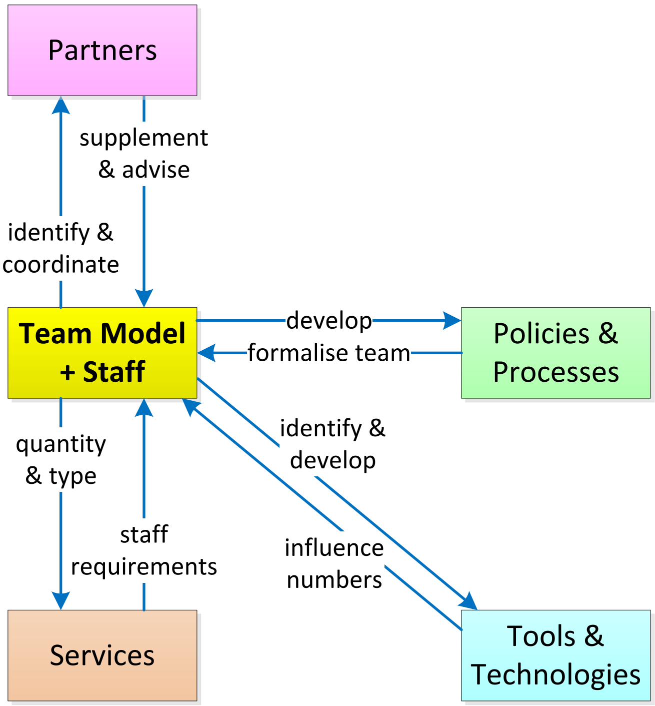


Figure 9.12: Links to/from People

As shown in figure 9.12, chapter 8 highlighted the following relationships to/from People:

- People *develop* Processes which *formalise the team* (including roles and responsibilities) (section 8.1, page 106).
- People *identify and develop* Tools and Technologies which in turn *influence* the required staff *numbers* (reducing load by automating tasks for example) (section 8.3, page 109).
- People (and their associated skills, experience, etc.) affect the *quantity, type and depth* of Services that can be provided. The selected Services will, on the other hand, dictate *staff requirements* (numbers and skills) (section 8.3, page 109).
- People *identify and coordinate* Partners who conversely *supplement and advise* staff (providing expertise and supporting the provision of services) (section 8.4, page 113).

The following section develops the part of the model centred around policies and processes.

9.3.2 Policies & Processes

Figure 9.13 highlights policies and processes in the CSIRT framework for development. Services and partners are further developed in parallel with policies and processes.

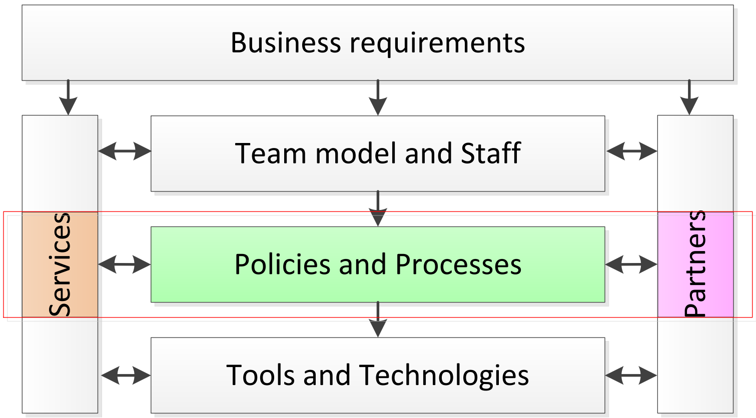


Figure 9.13: Framework for development: Policies & Processes

Chapter 5 introduced and detailed the major CSIRT policies and processes required for establishment and operations. Policies were defined as the higher-level governing principles implemented by processes (series of activities or steps). While establishing a CSIRT, policies and processes should be developed for operations.

This can be initiated with a policy template as per table 5.1 (page 62). Relevant policies for the specific CSIRT should then be identified and developed by CSIRT staff (as shown in figure 9.12). Sections 5.1.2 and 5.1.3 (pages 61 and 66) provide guidance for fundamental and secondary policies which should be developed as appropriate.

Section 5.2.2 (page 67) provided a generic incident handling process. This process should be tailored for the specific CSIRT environment and services. If the alerts, warnings and announcements services are provisioned, the information distribution process will be a useful addition (figure 5.3, page 72). Supplementary processes (like those in table 5.5, page 74) can be developed as needed.

Policies and Processes links to the other Ps

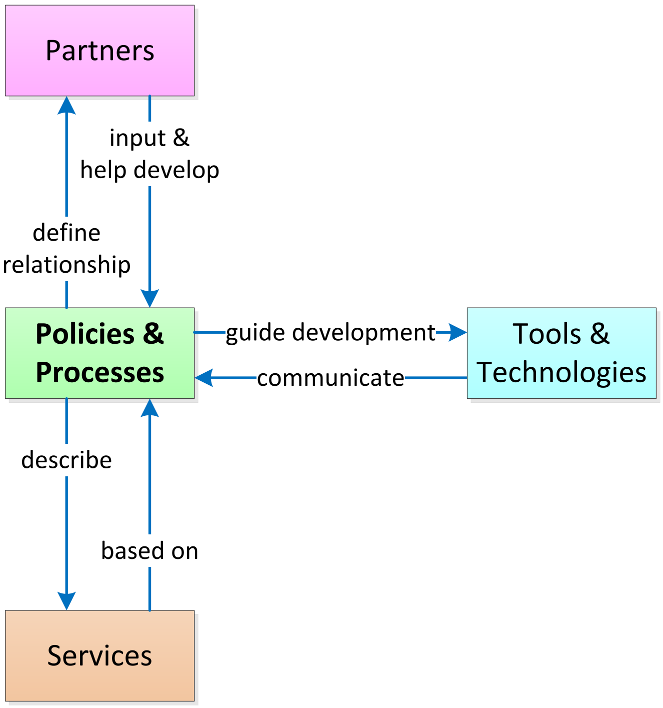


Figure 9.14: Links to/from Policies & Processes

The association between People, and Policies and Processes was already shown in figure 9.12. Chapter 8 highlighted the following additional relationships to/from Policies and Processes (figure 9.14):

- Policies and Processes *define the relationship* (cooperation agreements, service levels and reporting requirements) with Partners. Partners in turn are consulted for *input when developing* Policies and Processes (section 8.5, page 115).

- Policies and Processes *describe* Services (including service definitions, how they provided, priorities, etc.). Thus, Services are *based on* Policies and Procedures (but may be selected before) (section 8.6.1, page 117).

- Processes *guide the development* (design, configuration and management) of Tools and Technologies. These Tools and Technologies are subsequently used to *communicate* the Policies and Processes to the constituency and partners (sections 8.6.2 and 8.6.3, page 118).

The next section develops the tools and technologies part of the model.

9.3.3 Tools & Technologies

Figure 9.15 highlights Tools and Technologies in the framework for development.

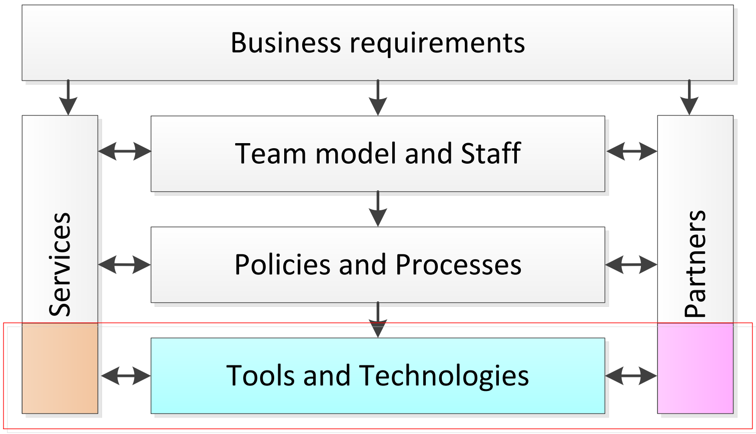


Figure 9.15: Framework for development: Tools & Technologies

Tools and technologies that may be relevant to the CSIRT are described in section 6.2 (page 82). The main ones should be obtained and/or developed as part of establishing a CSIRT. From table 6.2 (page 84), these are

- communication mechanisms;
- cryptographic mechanisms;
- an incident tracking/ticketing system and database;
- incident handling, analysis or security tools;
- general hardware and software;
- network and security devices;
- system administration tools; and
- a contacts database (or CRM system).

Tools and technologies are associated with People, and Policies and Processes as shown in figures 9.12 and 9.14 respectively.

In addition to these, section 8.2 highlighted the following link between Services, and Tools and Technologies:

- Services *determine* the Tools and Technologies which are *required for* providing said services (page 108). This link is shown in figure 9.16.

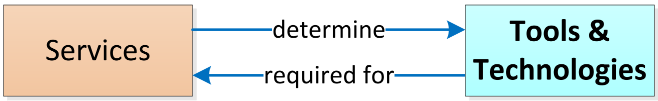


Figure 9.16: Link between Services and Tools & Technologies

Together, the links show that

- People are required to develop or obtain Tools and Technologies.
- Policies and Processes guide the development of Tools and Technologies.
- The definition of Services is required in order to know which Tools and Technologies are needed.

Thus, core staff and services selection are *prerequisites* to establishing the required tools and technologies. Additional staff requirements are influenced by the capabilities of supporting tools and technologies though, showing the iterative cycle between these two Ps (see figure 9.17).

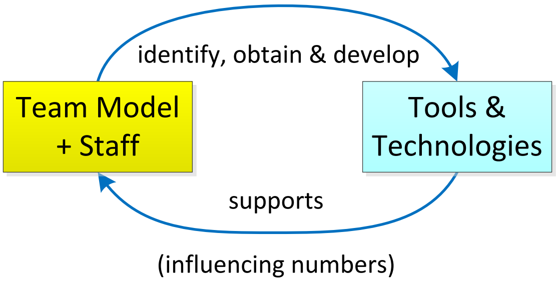


Figure 9.17: Iterative development cycle between People and Tools & Technologies (adapted from figures 8.6 and 9.12)

The final part of the model, the links around partners, are developed next.

9.3.4 Partners

Chapter 7 argued that partners are required for collaboration in resolving incidents and information sharing. Access to partners varies greatly based on the CSIRT environment. If the CSIRT is hosted within an established parent organisation there may be multiple internal partners that can assist with CSIRT activities (e.g., legal council, human resources, marketing and finances). An independent CSIRT, on the other hand, may have to establish many more internal capabilities. This can have a significant effect on staffing (section 8.4, page 113). Required external partners are more dependent on the team model and services provided by the CSIRT.

Policies and processes provide guidelines and agreements for interactions with partners who can provide input to the development of these documents (section 8.5, page 115).

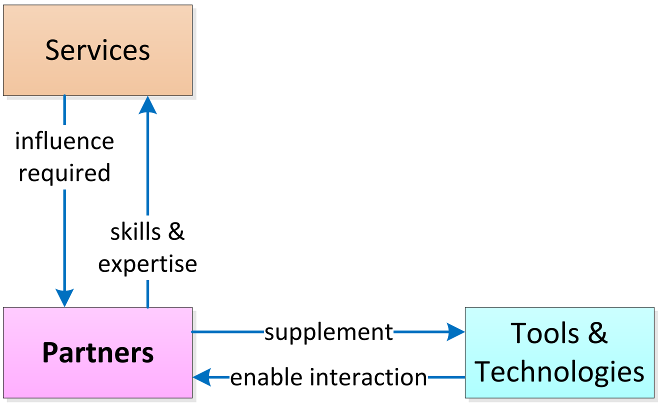


Figure 9.18: Links to/from Partners

Chapter 8 highlighted the following Partner relationships with Services, and Tools and Technologies (the other links have already been covered):

- Partners provide *skills and expertise* to Services, while the choice of Services *influences the required* Partner relationships (section 8.7.1, page 119).
- Partners can *supplement* Tools and Technologies. Some of these Tools and Technologies will *enable* Partner *interactions* and coordination (section 8.7.3, page 120).

These connections are shown in figure 9.18. Evidently, partners are integrated in all the other Ps and hence their position on the side of the framework (see figure 9.2).

9.4 Model for establishing a CSIRT

The previous sections, covering the business, services and four Ps requirements, can be combined to form a generic model for establishing a CSIRT. Together, these sections considered the following areas of CSIRT establishment:

- the environment,
- constituency,
- funding/budget,
- legal considerations,
- authority,
- services,
- team model and staff,
- policies and processes,
- tools and technologies, and
- partners.

For clarity, the model has been divided into two parts, the *strategic* view and the *tactical* view as described here.

9.4.1 Strategic view of the model

The *strategic* view is centred around the business requirements — those decisions that need to be made at the "higher" level. This view marks the entry point of the model, highlighting the initial decisions that must be made when proceeding to establish a CSIRT. These are

1. determining the *environment*,
2. figuring out who the *constituency* of the CSIRT will be, and
3. selecting a suitable *funding* model.

The strategic requirements are shown in figure 9.19. Only once these decisions are made can the rest of the requirements be met.

Authority and legal considerations have been included in this view as they can be directly determined from the definitions of the environment and constituency. They complete the business requirements and also have no direct relationship to the four Ps requirements in this model. For clarity, the effects of funding on the other areas of requirements, namely, services, people, and tools and technologies, have been included in the strategic view as the material "resource" for equipping the CSIRT. Besides the influence these other areas have on determining the budget, including them also simplifies the tactical model which is presented next.

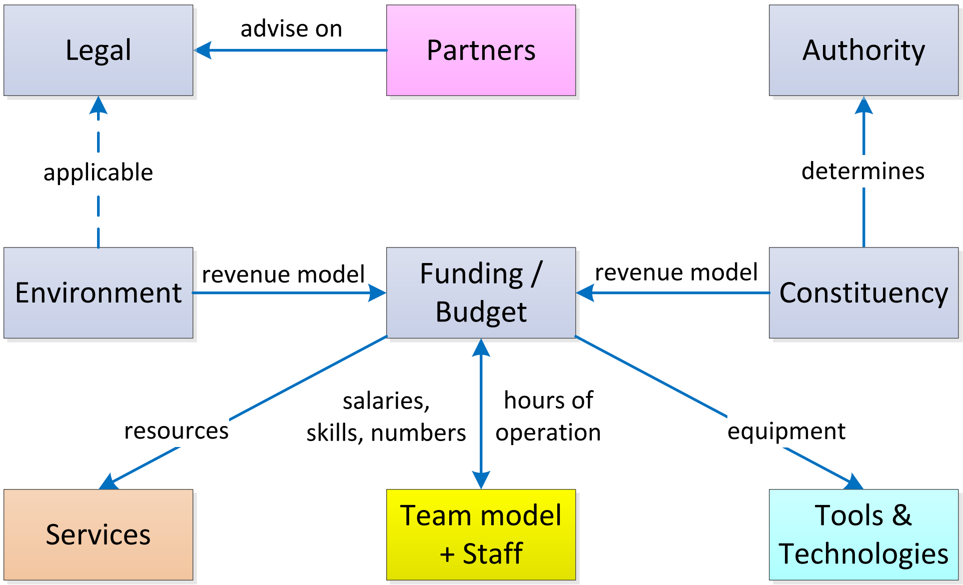


Figure 9.19: Strategic view of the model for establishing a CSIRT

9.4.2 Tactical view of the model

The remaining relationships, those between the four Ps, together with the environment, constituency and services, comprise the *tactical* view of the model. This presents the "how" part of establishing a CSIRT. The tactical view, showing these relationships, can be seen in figure 9.20. When establishing a CSIRT, both of these parts must be considered together to complete the model.

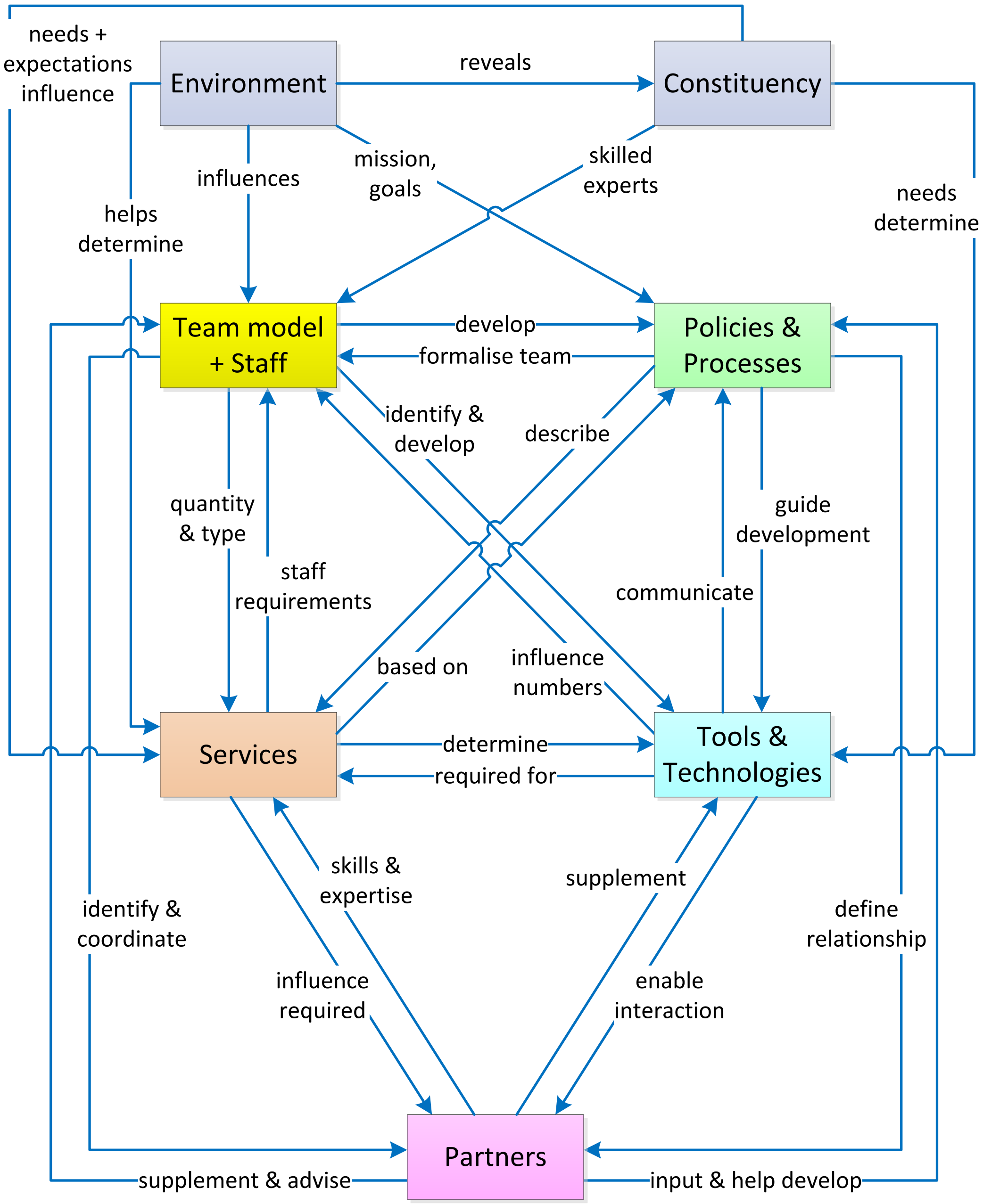


Figure 9.20: Tactical view of the model for establishing a CSIRT

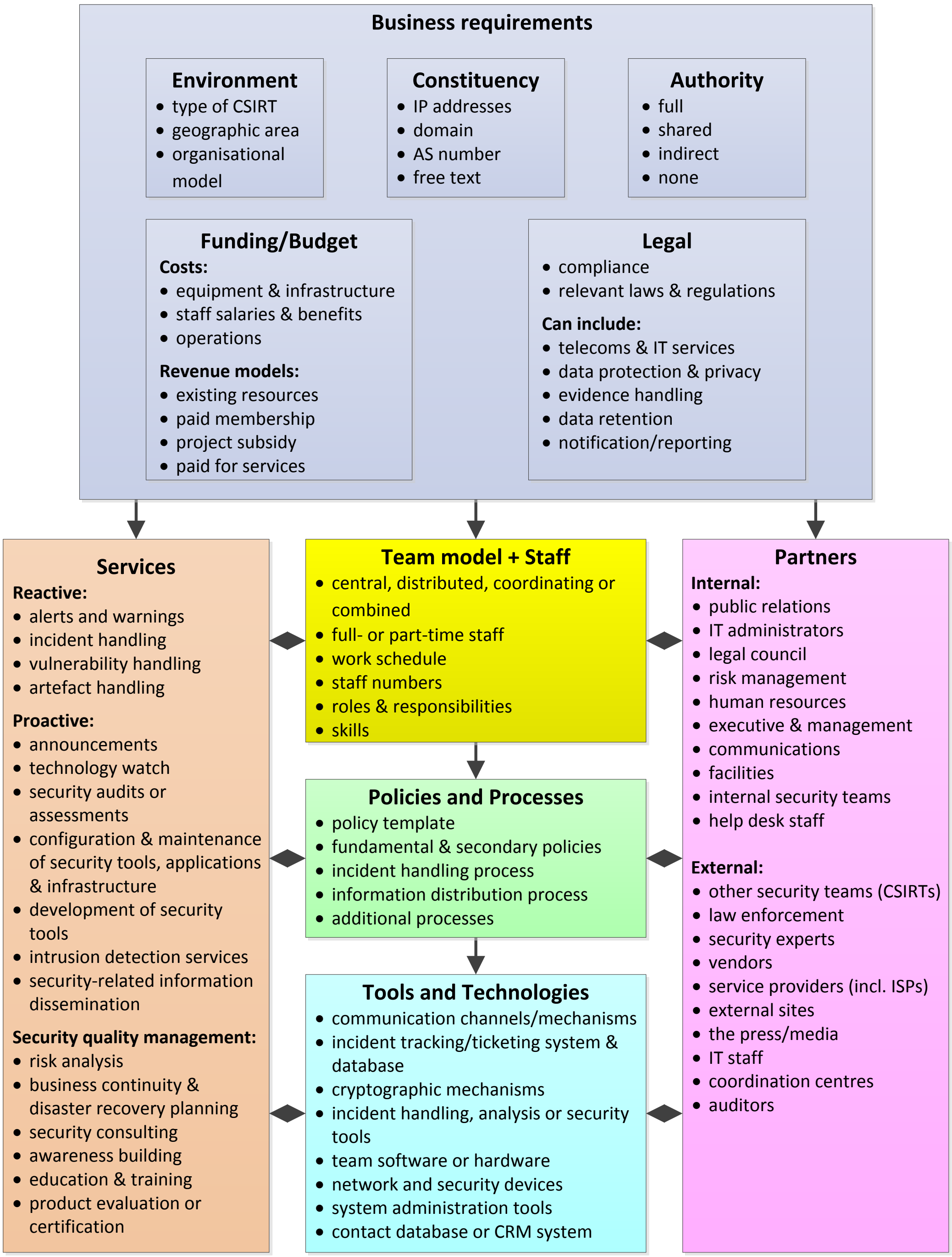
9.5 Conclusion

This chapter brings together the requirements and relationships from the previous chapters in the form of a generic model for establishing a CSIRT. This is the primary artefact and output of this research. To develop the model, it was necessary to progress through each area of the framework in turn highlighting the links to the other areas. Under each area, the specific decisions that needed to be made were conveyed. These decisions, together with the associations (influencers and dependencies) between the areas were brought together to develop the model holistically, ensuring that all requirements were included and in the correct order.

These decisions are summarised in figure 9.21. Firstly, the business requirement decisions need to be made. These include determining the environment, constituency, authority, funding and legal considerations applicable to the CSIRT. Following that, the services, team model and staffing, and partner decisions can be made. Next come policies and processes and then tools and technologies (with further developments in services and partners as applicable). The specific choices, options and required outcomes for each area are shown in the figure.

Following this model and addressing the decisions should produce a complete design for a CSIRT facilitating its implementation. This is demonstrated in the subsequent chapters by applying the model in the SA NREN environment.

To define the CSIRT capability, a needs analysis and requirements definition should be performed. These inputs may come from stakeholders, business needs, standards and best practices (Alberts et al., 2004, p. 54), and may be industry-specific. As a specific case study for an NREN CSIRT, the next chapter looks at the present situation in the SA NREN and identifies the need for a CSIRT through a survey presented to SANReN beneficiaries. This provides the required background for demonstrating the model in the SA NREN environment.



Business requirements

Environment
- type of CSIRT
- geographic area
- organisational model

Constituency
- IP addresses
- domain
- AS number
- free text

Authority
- full
- shared
- indirect
- none

Funding/Budget

Costs:
- equipment & infrastructure
- staff salaries & benefits
- operations

Revenue models:
- existing resources
- paid membership
- project subsidy
- paid for services

Legal
- compliance
- relevant laws & regulations

Can include:
- telecoms & IT services
- data protection & privacy
- evidence handling
- data retention
- notification/reporting

Services

Reactive:
- alerts and warnings
- incident handling
- vulnerability handling
- artefact handling

Proactive:
- announcements
- technology watch
- security audits or assessments
- configuration & maintenance of security tools, applications & infrastructure
- development of security tools
- intrusion detection services
- security-related information dissemination

Security quality management:
- risk analysis
- business continuity & disaster recovery planning
- security consulting
- awareness building
- education & training
- product evaluation or certification

Team model + Staff
- central, distributed, coordinating or combined
- full- or part-time staff
- work schedule
- staff numbers
- roles & responsibilities
- skills

Policies and Processes
- policy template
- fundamental & secondary policies
- incident handling process
- information distribution process
- additional processes

Tools and Technologies
- communication channels/mechanisms
- incident tracking/ticketing system & database
- cryptographic mechanisms
- incident handling, analysis or security tools
- team software or hardware
- network and security devices
- system administration tools
- contact database or CRM system

Partners

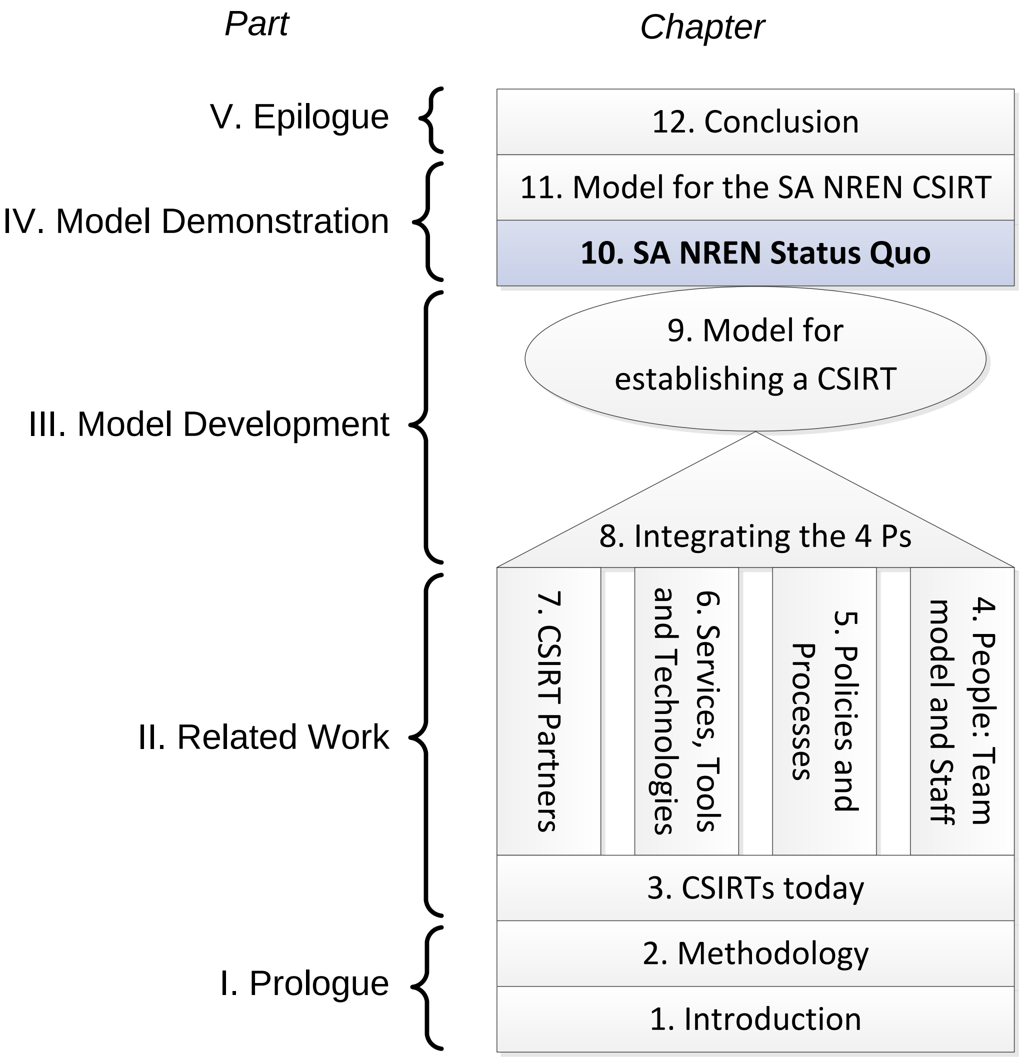
Internal:
- public relations
- IT administrators
- legal council
- risk management
- human resources
- executive & management
- communications
- facilities
- internal security teams
- help desk staff

External:
- other security teams (CSIRTs)
- law enforcement
- security experts
- vendors
- service providers (incl. ISPs)
- external sites
- the press/media
- IT staff
- coordination centres
- auditors

Figure 9.21: Summary of the decisions required for establishing a CSIRT

Part IV

Model Demonstration


Part
Chapter
V. Epilogue
12. Conclusion
IV. Model Demonstration
11. Model for the SA NREN CSIRT
10. SA NREN Status Quo
III. Model Development
9. Model for establishing a CSIRT
8. Integrating the 4 Ps
II. Related Work
7. CSIRT Partners
6. Services, Tools and Technologies
5. Policies and Processes
4. People: Team model and Staff
3. CSIRTs today
I. Prologue
2. Methodology
1. Introduction

Chapter 10

SA NREN Status Quo

The previous chapter defined a generic model for establishing a CSIRT. In order to apply the model in a specific context, is it useful to determine the current state of affairs with respect to incident response in that environment. This chapter describes the status quo of the incident response capability within the South African NREN as a case study. The results of a survey intended to collect data on the present situation are conveyed as a means to achieve this. This survey will investigate the need for a CSIRT from the perspective of the SA NREN community; in addition, it will reveal existing formal/informal incident response teams in the community (providing input to the CSIRT structure). Furthermore, beneficial CSIRT services are identified through a needs analysis.

Determining what the SA NREN environment looks like is the primary objective of this chapter. More specifically, the survey seeks to answer the following questions:

1. Does the community (possible constituency) need a CSIRT?
2. What existing security teams/mechanisms are in place (if any)?
3. Which skills and expertise do these teams have?
4. What kinds of malicious activity affect the users of the SANReN network?
5. Which CSIRT services will be most beneficial to the community?
6. How useful will an SA NREN CSIRT be?

The answers to these questions provide the background required for applying the generic CSIRT model in the SA NREN environment.

10.1 Method and instrument

Surveys are a excellent method for obtaining facts and opinions (Hofstee, 2006, p. 122). Therefore a *survey* was selected as the research method to answer the questions from the introduction. As the respondents completed the list of questions themselves, the research instrument is more specifically a *questionnaire* (Olivier, 2008, p. 81).

Following the study completed in the literature review (chapter 3), the information required prior to establishing a CSIRT was extracted from these sources and combined to form a meaningful questionnaire.

Google Docs (now Google Drive[1]) was chosen to host the questionnaire for the following reasons:

- It is provided as a free, electronic service.
- Forms (an extension of Google Sheets) provide a quick and easy means to create a survey by using standard fields and populating a spreadsheet in the background[2].
- The field types provided were sufficient to represent the desired questions in a suitable format.
- Access of results is restricted to the form owner (who can choose to share it if desired) — respondents can only see the questions.
- It is securely protected using HTTP over SSL/TLS (HTTPS).
- Live results are available from the first respondent.
- Automated graphical representation of results and summaries is included.
- Results can easily be exported for further analysis and graphing.
- The form and results are stored in the cloud — providing redundancy.

Using Google Forms and Sheets[3] further facilitated easy electronic distribution via email with a shared link.

[1] `https://drive.google.com`

[2] `https://www.google.co.za/edu/training/tools/drive/level1.html`

[3] `https://docs.google.com/spreadsheets`

10.2 Questionnaire

The main sections of the questionnaire and the information they are intended to gather are

Basic information

Information on the respondent and institution represented, including the number of users.

Security survey

Information on the nature of the security officer/team or, if there is not a team, how incidents are currently handled at the institution. In addition, the level of training of staff members is requested.

Network monitoring and malicious activity

Information on network monitoring and current types of malicious activity experienced at the institution. Whether the institution has an information security policy is also determined.

SANReN / TENET CSIRT

Information on whether the institution can benefit from the services of a CSIRT and which services would be most useful (in the opinion of the respondent).

In closing

Concluding information used to determine the willingness of the institution to participate in the initial phases of SA NREN incident response team establishment.

The complete questionnaire as used for the survey is available in appendix D (page 238). Relevant questions are highlighted in the following sections. To encourage honest responses, anonymity was promised via a privacy statement in the survey introduction (Olivier, 2008, pp. 81–82). For additional data reliability, options such as “other”, “unknown” and “maybe” were provided where meaningful (these responses were either excluded from the results or labelled accordingly). Furthermore, the raw data was suitably handled to preserve confidentiality and sensitive data was sanitised prior to publication.

10.2.1 Measurement types and techniques

The following types of measurement (and related techniques) were used in the questionnaire (Olivier, 2008, pp. 82–84):

- nominal measures — a list of alternatives with no specific order (e.g. the questions with radio buttons where only one answer can be selected);
- ratio measure — where zero has no meaning (e.g. "How many people in the team?");
- Likert scale — for the question on how useful a CSIRT would be to the respondent's institution;
- closed questions — most questions had restricted options for answers (although generally an "other" option was also provided); and
- open-ended questions: for "other" descriptions and comments (these were not utilised in the data analysis).

These measures and techniques provide a means to quantify the results in the following sections.

Lastly, prior to distributing the survey, Prof. R. A. Botha and staff from SANReN were asked for comment; their feedback was incorporated into the questionnaire.

10.2.2 Population and sample

The survey was designed and distributed in the 2012 calendar year. At the time there were 60 SANReN beneficiary institutions consisting of 27 science/research councils, 26 universities and seven supporting organisations[4]. This represents the *population* for the survey.

Out of this population, a *sample* of 49 institutions was selected to participate in the survey (i.e. for distribution). These were institutions actively using the SANReN network (i.e. with a status of "Connected"). Some supporting institutions were excluded as they are seen as partners rather than direct beneficiaries of the network (e.g. the South African State Information Technology Agency (SITA) and Teraco).

[4] The numbers were obtained from the SANReN contacts database — note that these are institutions and not sites and that institutions can have one or more site(s).

The 49 institutions include 23 universities, 23 science/research councils and three supporting institutions. These provide a fair representation of the SA NREN CSIRT constituency. Attempts were made to obtain a response from all 49 institutions in order to avoid bias and guarantee randomness of the sample. For reliability, the institution was requested to nominate a security contact from the IT department who would be able to answer the questions as accurately as possible.

10.2.3 Distribution and responses

Technical contacts and IT directors (where necessary) from each institution were phoned to introduce the survey and ask if they would be willing to participate. If so, they were asked to nominate the most suitable person to complete the survey (usually the IT security expert from the IT department (who could be the original contact)). Emails were sent to these "security contacts" with a brief introduction and link to the survey. This was followed up with reminder emails during the duration of the survey (targeted at those participants who had not yet responded). The initial survey was run from May-September 2012 and received 20 responses.

In order to elicit more responses, the survey was run again from November 2012 to February 2013. A further 17 responses were received, bringing the total number of respondents to 37 (out of 49 targeted institutions). Eighteen science councils, 16 universities and three supporting organisations completed the questionnaire. This subset is 76% of the sample and is therefore a sufficient, majority representation. Furthermore, it is balanced with respect to the proportion of science/research institutions to universities (1.125:1 with an original sample target of 1:1).

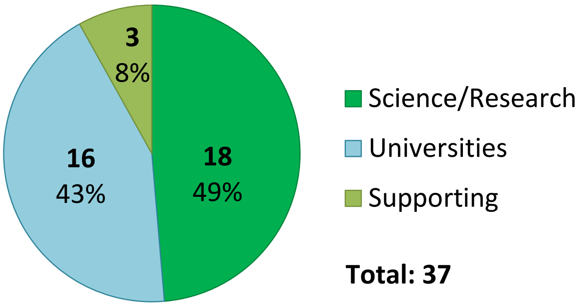


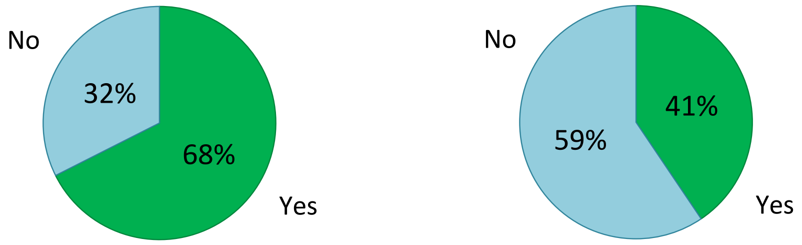
Figure 10.1: Survey respondents

10.3 Survey results

The previous sections explained the methodology used to gather the survey data as well as the questionnaire format and number of responses received. This section reveals the results of the survey with graphical representation where appropriate. (Note that percentages have been rounded to the nearest digit.)

10.3.1 Staff and dealing with incidents

The 37 institutions that responded represented 420 684 users in 2012. Sixty-eight percent of these respondents have some sort of security team (figure 10.2a); but only 41% of the total respondents' staff have formal training in information security (figure 10.2b).



(a) Respondents with security teams (b) Staff with formal training

Figure 10.2: Security teams and training

The average number of team members is 2.64 with the least being one security officer and the most six members (possibly part time). Ten out of the twelve respondents who do not have a security team nominate a responsible person from the IT department at the time of the incident.

10.3.2 Network monitoring and malicious activity

Eighty-one percent of respondents monitor their network and/or computers for malicious activity. The types of malicious activity affecting institutions in 2012 are shown in figure 10.3.

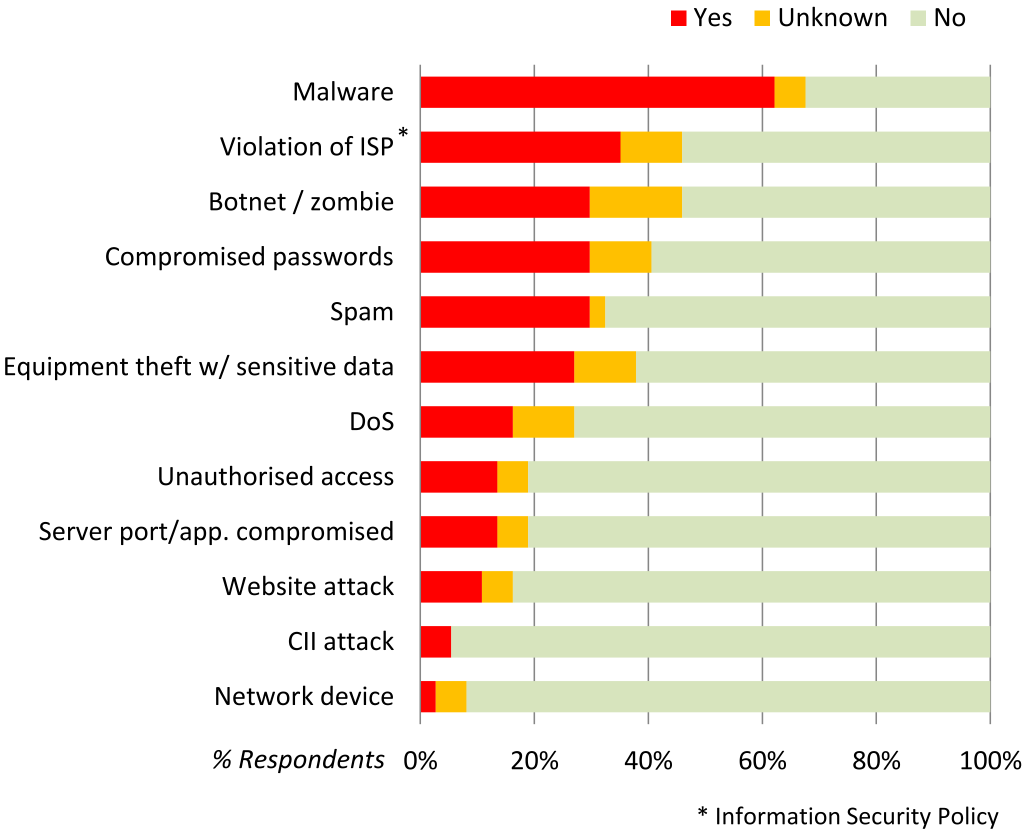


Figure 10.3: Incidents affecting respondents

Malware (viruses, worms, trojans, etc.) was clearly the most prevalent with more than 60% of respondents affected by it. Violation of the Information Security Policy (ISP) was the next highest (35%); this makes sense as any malicious activity (computer security incidents) should violate the information security policy (it was perhaps not the highest because only 68% of respondents have an information security policy (3 were busy developing one at the time)). Botnet / zombie infections, password compromises and spam are tied for third place (30% affected) (not counting the respondents who did not know). Observing that the question on spam requested a "no" response for spam that is successfully filtered, this is an interesting outcome considering the abundance of anti-spam solutions on the market. The number of "unknown" responses could also be a cause for concern particularly for incidents like compromised passwords, sensitive data on stolen equipment and website attacks (although this answer could also indicate that the respondent was not willing to share that information).

10.3.3 SA NREN CSIRT: Benefit and useful services

Thirty-one respondents (84%) indicated that they would definitely benefit from an SA NREN CSIRT. Four respondents were unsure with only two respondents indicating they that did not believe they would benefit from a CSIRT (figure 10.4).

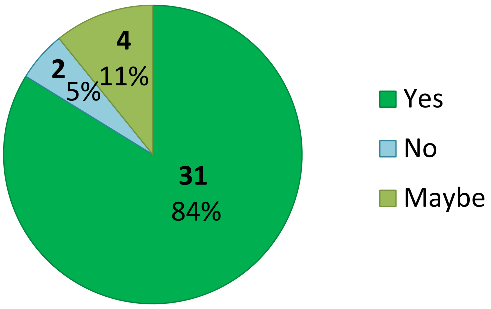


Figure 10.4: Institutions that would benefit from an SA NREN CSIRT

In addition, using a rating system from 1 (not useful) to 10 (very useful), 76% of respondents indicated that a CSIRT would be more than useful to them (i.e. selected 6 or more out of 10) with an average of 7.4 across respondents (figure 10.5). The most useful services to the respondents are shown in figure 10.6.

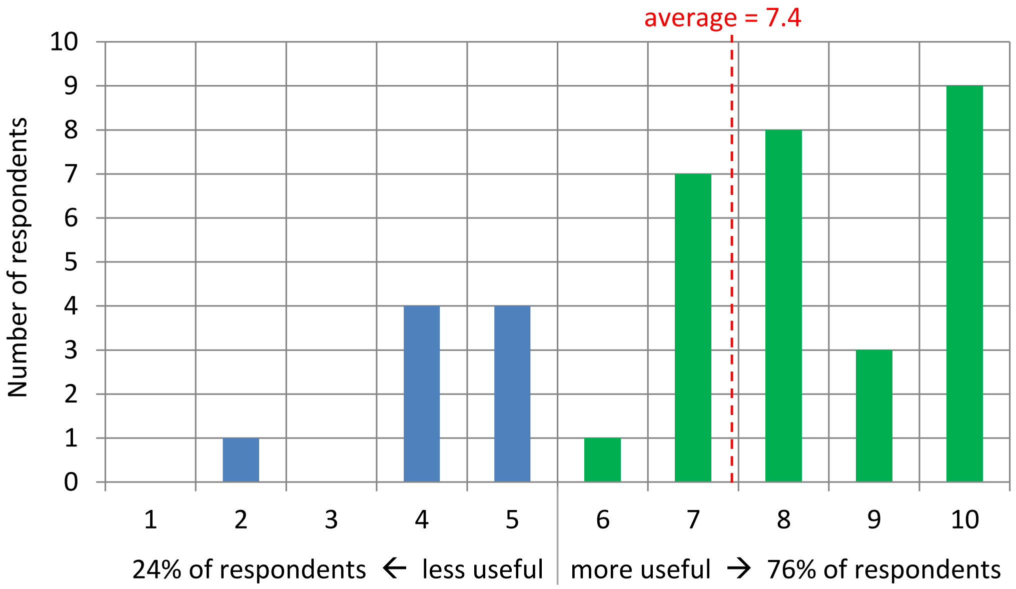


Figure 10.5: How useful would an SA NREN CSIRT be?

Interestingly, the results show that the traditionally proactive CSIRT services are the ones that will be most useful to the constituency. The top three services (selected as "useful" by 30 out of 37 respondents) are

- alerts and warnings,
- training, and
- security education.

Security consulting/recommendations comes in next, closely followed by vulnerability reporting and handling and security audits/assessments. Incident response on site is the least interesting service to the community with less than 50% finding it useful.

10.4 Discussion and limitations

From the "most useful services" results, it can be seen that proactive services will be most effective in helping the constituency reduce incidents. These should therefore be given primary focus. Of course, the standard incident response services (those which actually define a CSIRT) cannot be ignored and will be supplemented by these proactive services as a core offering.

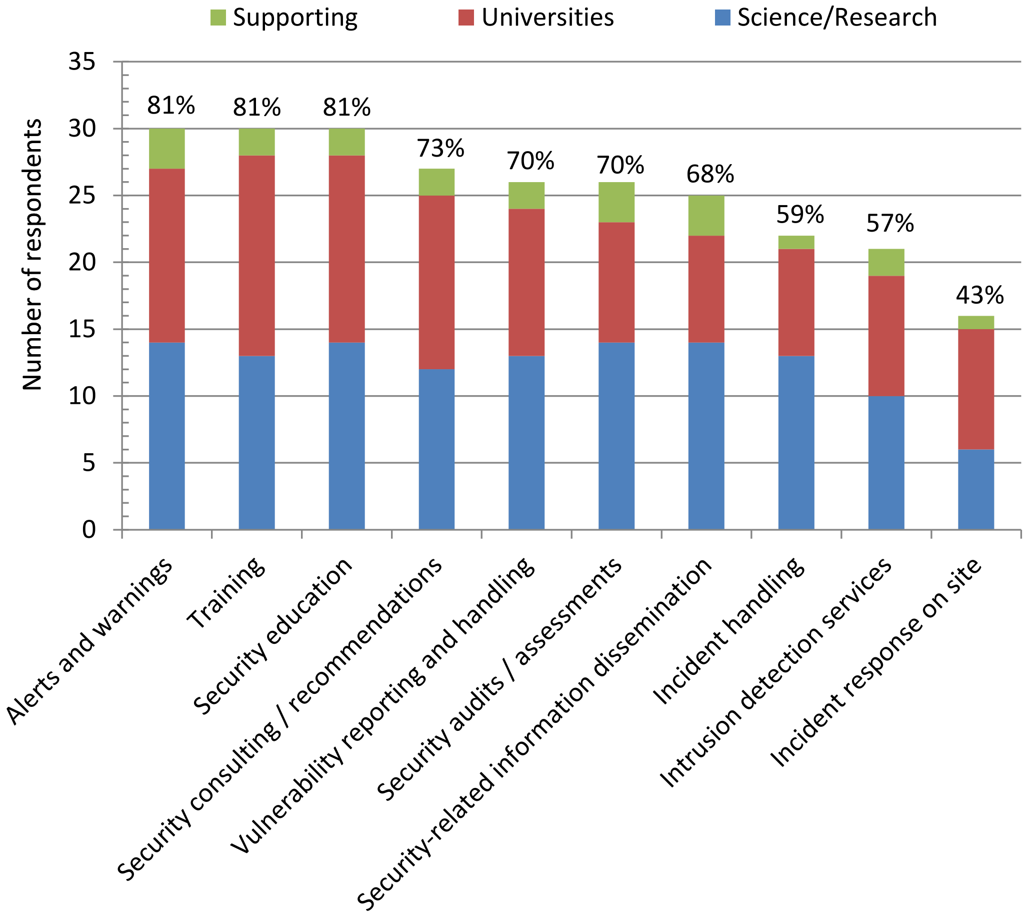


Figure 10.6: Most useful services

No clear correlation was found between the type of institution (science/ research, university or supporting) and the other answers (e.g. whether or not they had a security team, training, monitoring or even an information security policy) except for the most useful services. The answers for science/ research institutions and universities are shown in figure 10.7 (supporting institutions were excluded due to the low number of respondents although they are included in the total). The top four services for each are indicated with arrows.

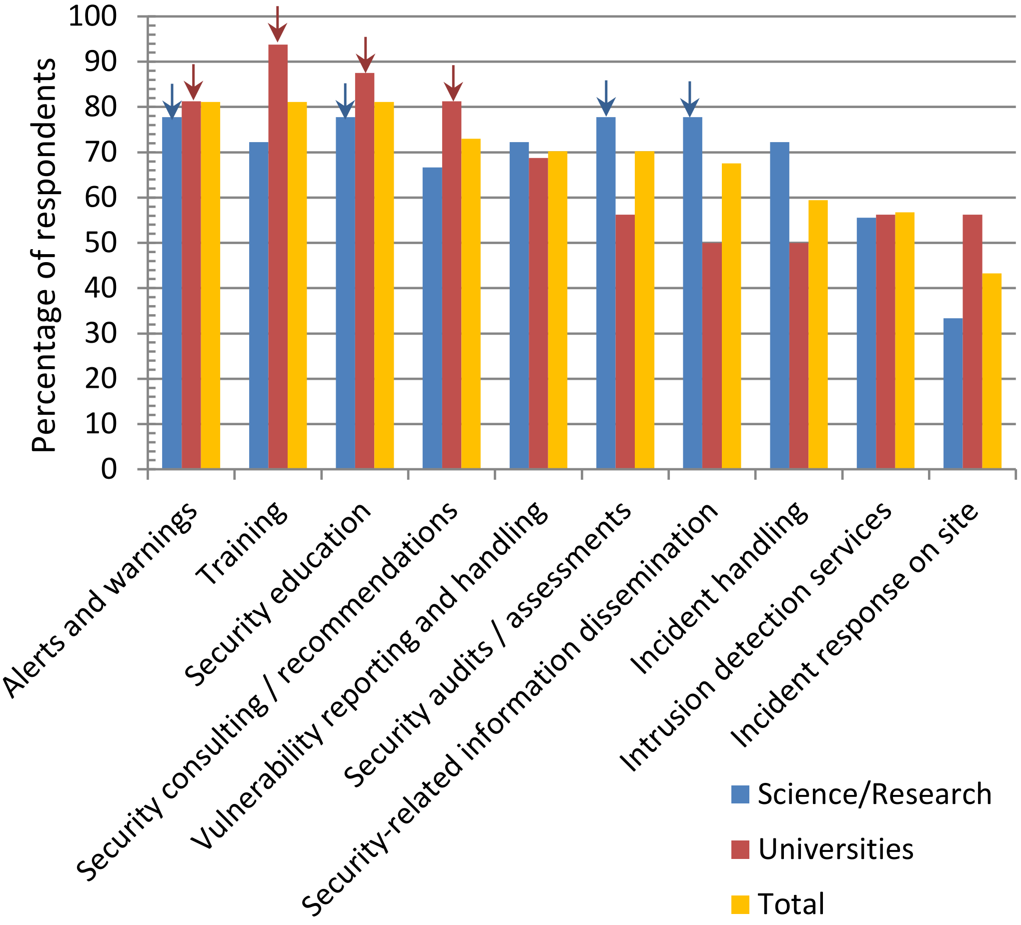


Figure 10.7: Useful CSIRT services by institution type

The following can be observed from the graph:

- Universities' top four useful services match the total top four useful services.
- Security audits/assessments and information dissemination are quite important to science/research organisations but not universities (of the lowest in fact for universities).
- The usefulness of vulnerability reporting and handling as well as intrusion detection services are very close for both types of institutions. The total responses can therefore be used to represent both groups for these services.
- Caution should be exercised when considering the provisioning of services with extremes in usefulness between institution types (i.e. security audits/assessments, information dissemination, incident handling and response on site services). Specific types of institutions (those that find it more useful) should possibly be targeted first for these services and the combined usefulness to the constituency should also be evaluated. Therefore these services should have a lower priority for the initial offering than others (confirming the focus on the top four to five useful services across the whole sample).

The limitations of this survey include the interpretation of questions (leading to possible ambiguity) and the lack of detail in responses (leading to reduced utility). As an example of the first limitation, what does the question "how many users at your institution?" really mean? Is it asking for the number of people physically on site, enrolled at the institution and/or supported by it? For example, one university reported 10 000 users but in 2011 had 328 864 enrolled students (DHET, 2013). How did the respondent interpret "users"?

Another example includes the type of security teams — what is the difference between a formal team and an informal one? Is a formal CSIRT one that is registered with FIRST (or a similar organisation), has a mission/charter or dedicated personnel? Is a security officer classified as formal or informal? This limitation could have been addressed by explicitly defining key terms and/or providing more specific options.

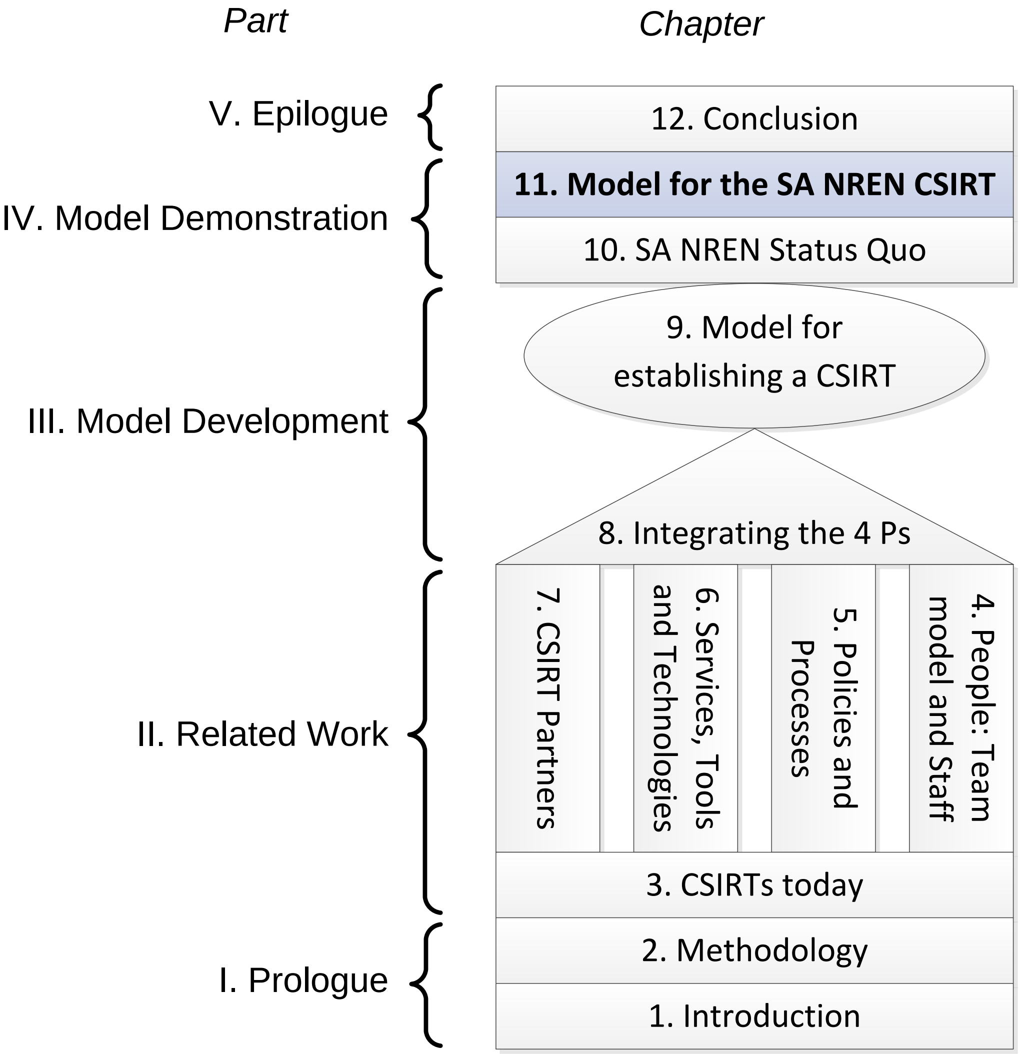
As an example of insufficient detail, the question on network/computer monitoring does not ask for any clarification. The only potentially useful result from this question is that 19% of respondents do not do any kind of monitoring. It would have been more useful if the extent of monitoring was known. This question could have been improved by asking more specifically which of the following mechanisms are used by the respondent's institution: centralised logging, intrusion detection systems, netflow analysis, etc. resulting in a more useful outcome regarding the state of affairs of network monitoring in the SA NREN environment.

Due to the limitations, the answers to these questions were not used in the analysis. Fortunately, none of them were critical to the research outcomes (and should probably therefore have been excluded in the first place).

10.5 Conclusion

This chapter presented the questions and results of a survey used to assess the status quo of incident response in the SA NREN (particularly the beneficiary institutions). The results showed the need for an SA NREN CSIRT as well as community support thereof. Proactive services were highlighted as most useful and thus revealed as the primary focus. The existence of a number of security teams in the community strengthens the argument for coordination. Furthermore, these teams could provide resources for the NREN team.

Chapter 11 builds on this chapter by integrating the findings with the generic model for establishing a CSIRT to design the capability for the SA NREN.


Part
Chapter
V. Epilogue
IV. Model Demonstration
III. Model Development
II. Related Work
I. Prologue
12. Conclusion
11. Model for the SA NREN CSIRT
10. SA NREN Status Quo
9. Model for establishing a CSIRT
8. Integrating the 4 Ps
7. CSIRT Partners
6. Services, Tools and Technologies
5. Policies and Processes
4. People: Team model and Staff
3. CSIRTs today
2. Methodology
1. Introduction

Chapter 11

Model for the SA NREN CSIRT

In chapter 9 a generic model for establishing a CSIRT was presented. The previous chapter conveyed the status quo of the SA NREN beneficiaries utilising the results of a survey to show the need for a CSIRT and the most useful services.

This chapter will bring these last two chapters together by applying the model to the SA NREN environment, showing the utility and effectiveness of the model. This is achieved utilising the framework presented in figure 9.2 (repeated in figure 11.1 for convenience).

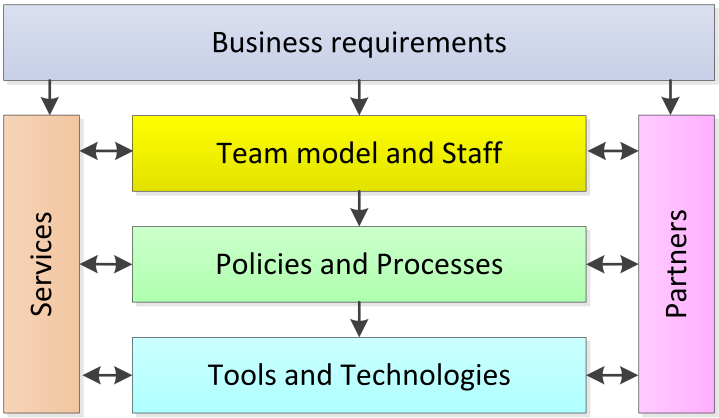


Figure 11.1: Framework for the CSIRT model (by author)

11.1 Phase 1: Business requirements

Phase 1 address the business requirements for the SA NREN CSIRT as shown in figure 11.2.

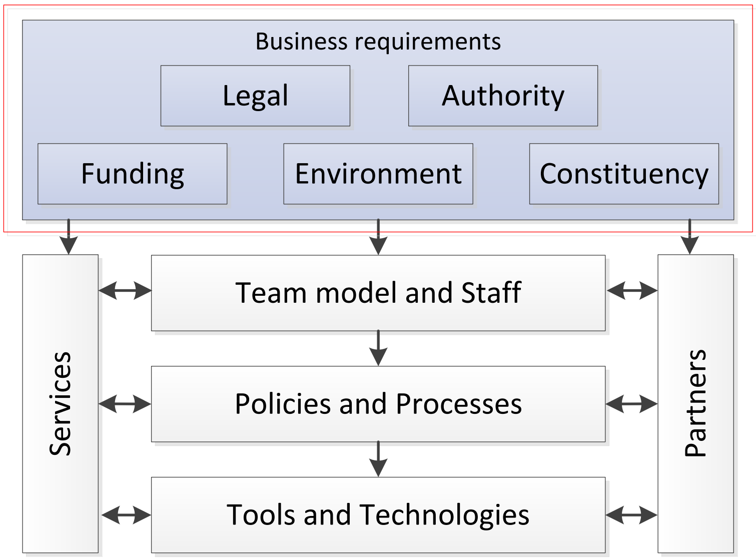


Figure 11.2: Phase 1: Business requirements for the SA NREN CSIRT

The SA NREN is constituted of two organisations, SANReN, who design and build the network, and TENET, who operate it (section 1.2, page 4). The SANReN competency area is hosted by the Meraka Institute of the CSIR. The team has access to shared services including human resources, finances, legal, facilities and other (section 11.2.3, page 180). SANReN employ 11 technical staff executing the design and roll-out of the network as well as value-added services development. These could potentially be involved in CSIRT activities together with management staff.

TENET is an independent non profit company governed by a board of directors from its stakeholders. "TENET secures global interconnectivity with other NRENs and with the Internet worldwide through the London and Amsterdam gateways of the UbuntuNet Alliance for Research and Education Networking" (TENET, 2013, para. 24). TENET run the SA NREN Network Operations Centre (NOC) internally but have outsourced 24x7 fault reporting and other help desk services (TENET, 2013). TENET additionally manage and administer the .ac.za domain as well as IPv4 and IPv6 address allocations for qualifying institutions. According to the CEO, TENET employ five network engineers and five NOC staff (including management) who could participate in or be affected by CSIRT activities.

11.1.1 Environment

Section 9.1.1 (page 129) provided a summary of the questions that need to be answered in order to determine the CSIRT environment; that is, the type of CSIRT, the geographic area and the organisational model. This section answers those questions for the SA NREN CSIRT and thereafter explores the subsequent outputs to the other areas as shown in figure 9.5 (page 130).

Based on the previous description of the environment, these questions can be answered as follows:

1. What *type* of CSIRT is it?

   The SA NREN serves the education and research institutions of South Africa. It is therefore an *academic sector* CSIRT.

2. What *geographic area* will be covered by the CSIRT?

   The beneficiaries of the network are the South African universities and science councils, thus the geographic area is the *country of South Africa*.

3. Which *organisational model(s)* will the CSIRT use?

   ENISA (2006, p. 23) argue that the *campus* model is mostly adopted by academic and research CSIRTs. The NREN CSIRT acts as the core CSIRT, coordinating the independent campuses and acting as a single point of external contact. This CSIRT provides the core services and information distribution to the campus teams (ENISA, 2006, p. 23). This choice of model is reinforced by the existence of security teams in 68% of the constituency motivating the need for coordination (see figure 10.2a, page 155).

   Considering that the SA NREN comprises two existing organisations, taking the CSIRT operational can be expedited by *embedding* it in one (or both) of the existing organisations. This will also simplify resource planning and procurement (from staff to finances and equipment). Additionally, members from the constituency can participate in team activities (aid in the provisioning of services). Therefore, an *embedded* model is proposed for the coordinating CSIRT. Elements from the campus model can be integrated where applicable. Where this SA NREN CSIRT fits into the CSIRT hierarchy is shown in figure 11.3.

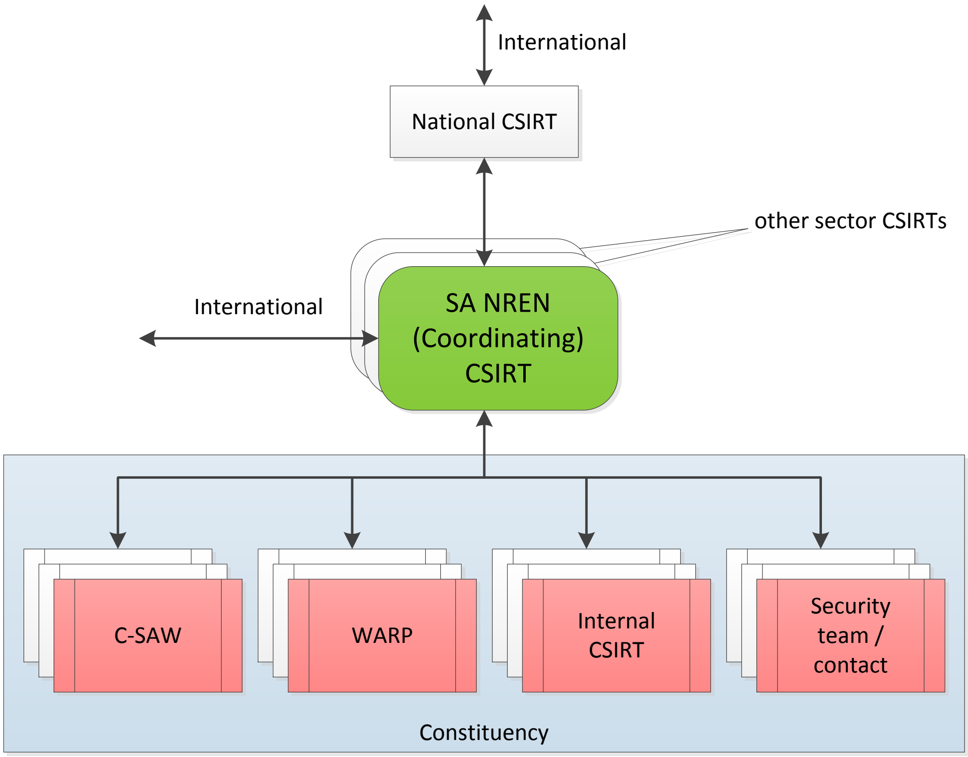


Figure 11.3: SA NREN CSIRT plus constituency teams (by author)

The effects on the other areas for consideration of these environmental decisions are as follows (shown in figure 11.4):

- Legal — the environment shows that the laws and regulations of South Africa are relevant to the CSIRT (more detail is provided later in this section).
- Constituency — the constituency is revealed as the beneficiaries (or sites connected to and receiving services from) the SANReN network (detailed definition provided next in section 11.1.2).
- Funding — the environment indicates two options for revenue, either the SANReN government funding or TENET cost recovery. These two options will be explored in section 11.1.2.
- Services — the environment hints that the services typically provided by a coordinating CSIRT will be the most relevant. This will be considered together with the needs and expectations of the constituency to determine the CSIRT services in section 11.2.2.
- Team model and staff — the nature of the environment indicates that a coordinating team model is the most suitable for this environment. More detail on the team model and staffing issues is presented in section 11.2.
- Policies and processes — the mission and goals emanating from the SA NREN CSIRT environment will serve as a foundation for the policies and processes in section 11.3.

The rest of this section discusses the mission and legal considerations related to the environment.

Mission

The mission statement communicates the goals and objectives of the CSIRT providing a basic understanding of what the team is trying to achieve (West-Brown et al., 2003, p. 10). The mission defines the basic purpose and function of the team in terms of the services it provides to the constituency (ENISA, 2006, p. 16; Killcrece et al., 2003a, p. 7).

As emphasized in the previous section, a preliminary mission needs to be defined due to the influence it has on the services, and policies and processes of the CSIRT (West-Brown et al., 2003).

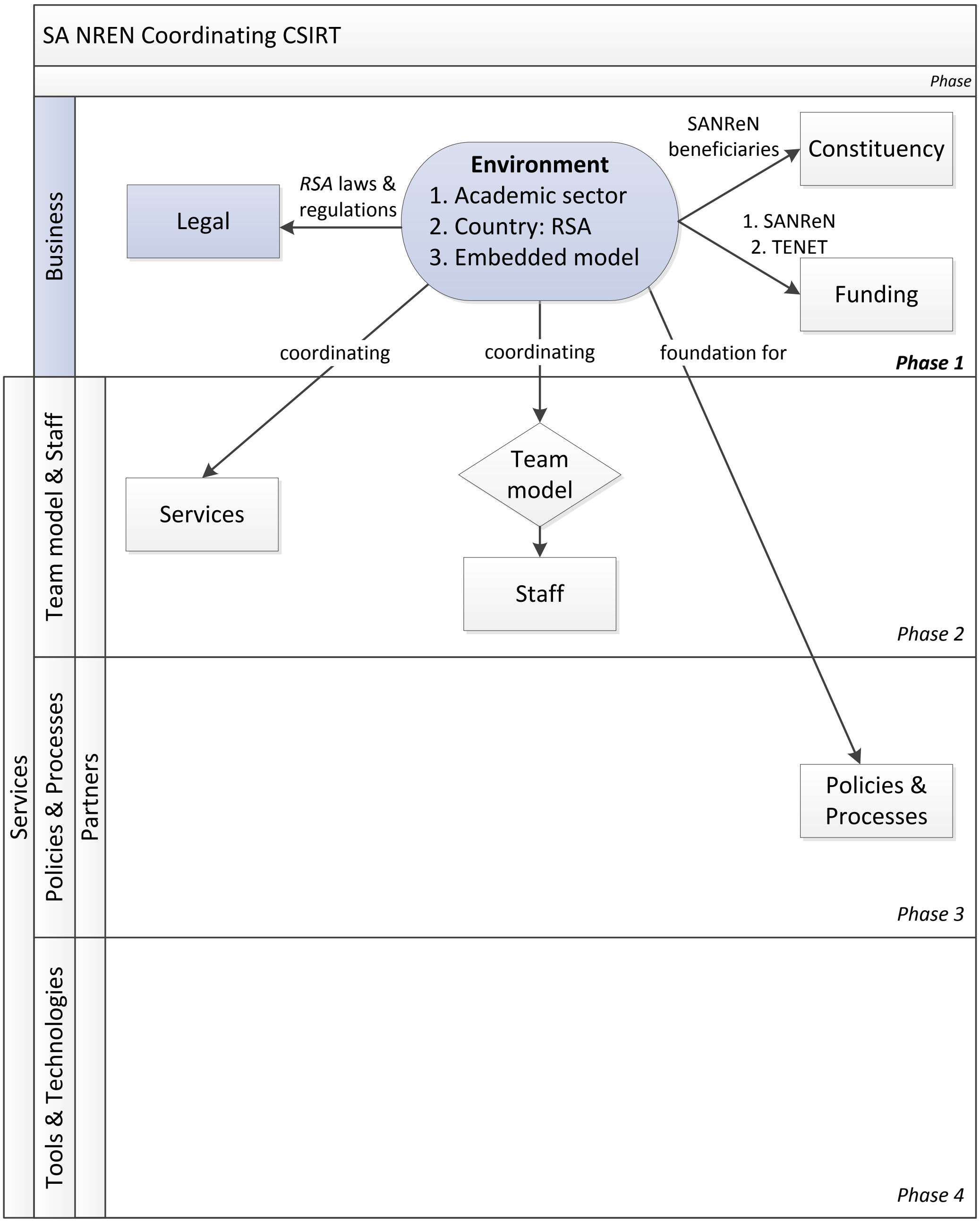


Figure 11.4: SA NREN CSIRT: Environment with links to other areas

To do this, the mission of the hosting organisation is used as a starting point (ENISA, 2010; West-Brown et al., 2003). Therefore, the objectives of SANReN and TENET are applicable (see section 1.2, page 4). To clarify this, "TENET's main purpose is to secure, for the benefit of South African universities and associated research and support institutions, Internet and Information Technology services"[1]. The primary *objective* of the SA NREN CSIRT therefore is:

> *to protect the SANReN network and its users from malicious activity (as far as practicable), without compromising on network performance, and to mitigate IT security incidents when they do occur.*

Based on this objective, the *mission* of the SA NREN CSIRT can be defined as:

> *to provide incident response coordination and proactive IT security services to the sites and users of the SANReN network; with the goal of minimising the occurrence of incidents, equipping the constituency to better safeguard against malicious activity and to coordinate the handling of incidents across the constituency with external parties.*

This mission provides some clues as to the constituency, services, policies and processes of the CSIRT as uncovered in the sections following the legal considerations.

Legal considerations

Table 11.1: Relevant South African legislation for the SA NREN CSIRT

Act/Policy	Link (verified 23 September 2014)
ECT Act	`http://www.gov.za/documents/download.php?f=68060`
RICA	`http://www.gov.za/documents/download.php?f=187367`
POPI Act	`http://www.gov.za/documents/download.php?f=204368`
Cybersecurity Policy	`http://www.gov.za/documents/download.php?f=117591`

[1] `http://www.tenet.ac.za/`

As the environment is the main input to the legal area, the design factors of the legal area can be considered here. For the SA NREN, the following laws and regulations for the Republic of South Africa are relevant (not intended to be an exhaustive list):

- the Electronic Communications and Transactions (ECT) Act 25 of 2002,
- the Regulation of Interception of Communications and Provision of Communication-related Information Act (RICA) 70 of 2002,
- the Protection of Personal Information (POPI) Act 4 of 2013, and
- the Cybersecurity Policy of South Africa (currently in draft form).

These acts and policy can be accessed through the download links provided in table 11.1.

Once partnerships have been established, the applicable sections from these laws and regulations can be integrated with policies and processes based on consultations with relevant internal and external specialists. This would form part of the bottom-up implementation.

11.1.2 Constituency

The constituency has been identified from the environment as the beneficiaries of the SA NREN (sites connected to SANReN and receiving services from TENET). These are formally defined in the TENET connection policy as “campuses of South African education and research institutions and associated support institutions in the public sector that connect to the network” (TENET, 2012b, p. 1). This can be regarded as the *free text* description. As indicated in section 3.2.1 (page 38), free text can be unclear making it difficult to determine if a host is part of the constituency or not. Additionally, indirect connections to SANReN by schools, Technical Vocational Education and Training (TVET) colleges, museums and others are allowed (TENET, 2012b). Thus further complicating the scope of the constituency.

In order to avoid ambiguity (and because the information is available) the constituency of the SA NREN CSIRT can be officially defined as the combination of the following:

1. hosts belonging to AS2018 (the Autonomous System number allocated to TENET),
2. the domain .ac.za, and
3. IP addresses in AS2018[2].

Together these clearly define the constituency and thereby provide the following inputs (see figure 11.5):

- Authority — all sites connecting to SANReN are required by TENET to sign an Acceptable Use Policy (AUP). Although the organisations are independent institutions, this AUP provides the CSIRT with limited authority to disconnect or restrict access from "misbehaving" sites (more information next).
- Funding — the constituency reveals that a cost recovery model could be considered for the SA NREN CSIRT. This will be elaborated on in section 11.1.2.
- Services — the nature of the constituency, including their needs and expectations, hints at the appropriate services (revealed in section 11.2.2).
- Team model and staff — considering that the constituency is comprised primarily of universities and research organisations, it is very likely that there are experts at these institutions who may be able to complement or support CSIRT staff. This is explored further in section 11.2.3.
- Tools and technologies — combined with the coordinating role of the CSIRT, the nature of the constituency highlights the most relevant tools and technologies (e.g. high bandwidth connections make various electronic mechanisms attractive) (see section 11.4).

Initially, CSIRT services can be provided to a subset of the constituency. This will allow for a phased approach without straining resources.

[2] available from: `http://www.cidr-report.org/cgi-bin/as-report?as=AS2018` or `http://bgp.he.net/AS2018#_prefixes`

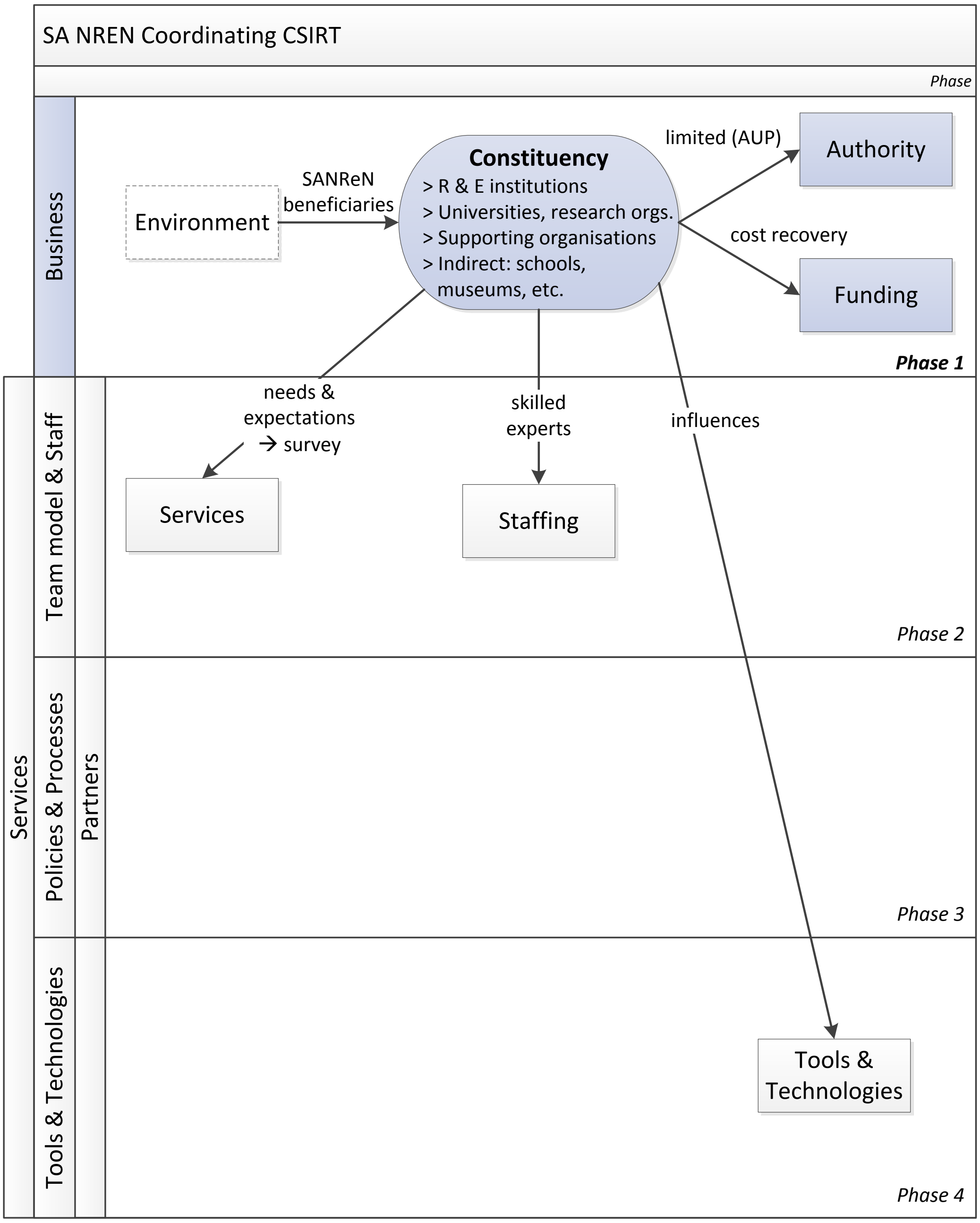


Figure 11.5: SA NREN CSIRT: Constituency with links to other areas

Authority

The constituency consists of independent (of SANReN/TENET) organisations connected to the SANReN network. This means that the SA NREN CSIRT will either have limited or no authority to enforce actions. The TENET AUP (TENET, 2012a) clarifies this by distinguishing between acceptable (legal) and unacceptable use of the SANReN network. Organisations connecting to SANReN must agree to this policy, with the result that it can be enforced. This means that the SA NREN CSIRT has *limited authority* whereby it can instruct a misbehaving site to act (rectify non-compliance) or face restricted access to or even disconnection from the network.

Funding

As indicated when uncovering the SA NREN environment (section 11.1.1), funds can be sought from both SANReN and TENET. According to the terms of the TENET/SANReN collaboration agreement, the SANReN Competency Area (CA) is responsible for developing advanced services which are then handed over to TENET for operations (TENET, 2013). As the SA NREN CSIRT can be regarded as an advanced service, this framework should apply. SANReN is funded by the Department of Science and Technology (DST) in 3 year cycles. Initial funding for establishing a CSIRT has already been approved in the SANReN budget and 2013–2016 business plan; i.e. *existing resources* or sources of funding (as per section 9.1.3, page 132) can be used to establish the CSIRT. Thereafter, once the CSIRT is operational, it should be handed over to TENET who become responsible for providing ongoing operational funding.

There are various approaches which TENET can use to recover costs. These can include one or more of the following:

- distributing the costs throughout the constituency by augmenting port or service charges (*project subsidy*),
- charging a fixed annual CSIRT service fee per site/institution (*paid membership*), and/or
- offering free basic CSIRT services and charging for premium services (*paid-for services*).

The determination of funding sources and the revenue model complete the considerations for the business requirements. The next phase looks at the People-related requirements.

11.2 Phase 2: Team Model and Staff

The next phase for establishing a CSIRT (following the business requirements) according to the generic model, is to design the team model and staff. Initial requirements for services and partners are commenced in parallel with this as per figure 11.6.

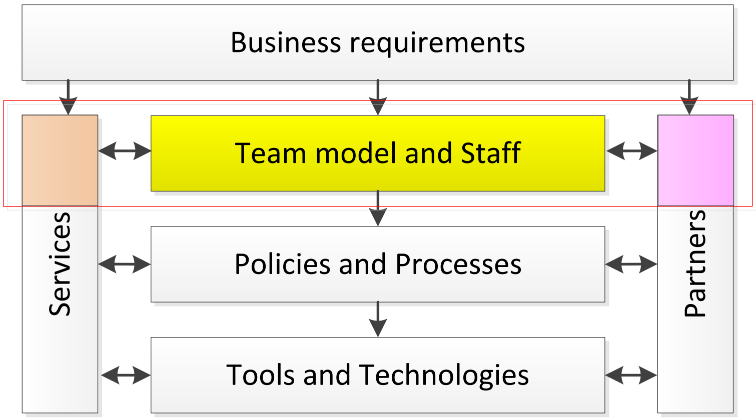


Figure 11.6: Phase 2: Team model and Staff for the SA NREN CSIRT

Section 9.3.1 (page 135) showed that the following need to be determined for the SA NREN CSIRT:

1. Team model — central, distributed, coordinating or combined (based on the environment and funding).

2. Staffing — which include determining

   - the work schedule,
   - whether full- or part-time staff are most appropriate,
   - the number of staff initially required (can be supplemented by the constituency and/or partners),
   - required staff skills (dependent on services selection and technologies in use by the constituency),
   - roles and responsibilities, and
   - the constitution of core and extended teams (based on the above as well as accessibility to internal partners).

These decisions are based on the environment, available funding, the accessibility of skilled experts from the constituency, services requirements and the selected team model.

Next, the team model is explored followed by the initial services selection and partners investigation to provide a background for staffing considerations.

11.2.1 SA NREN CSIRT team model

The SA NREN environment (section 11.1.1) provides direction for the team model. The combination of campus and embedded organisational models with a focus on coordination (as an academic sector CSIRT) suggests a team model structured as shown in figure 11.7.

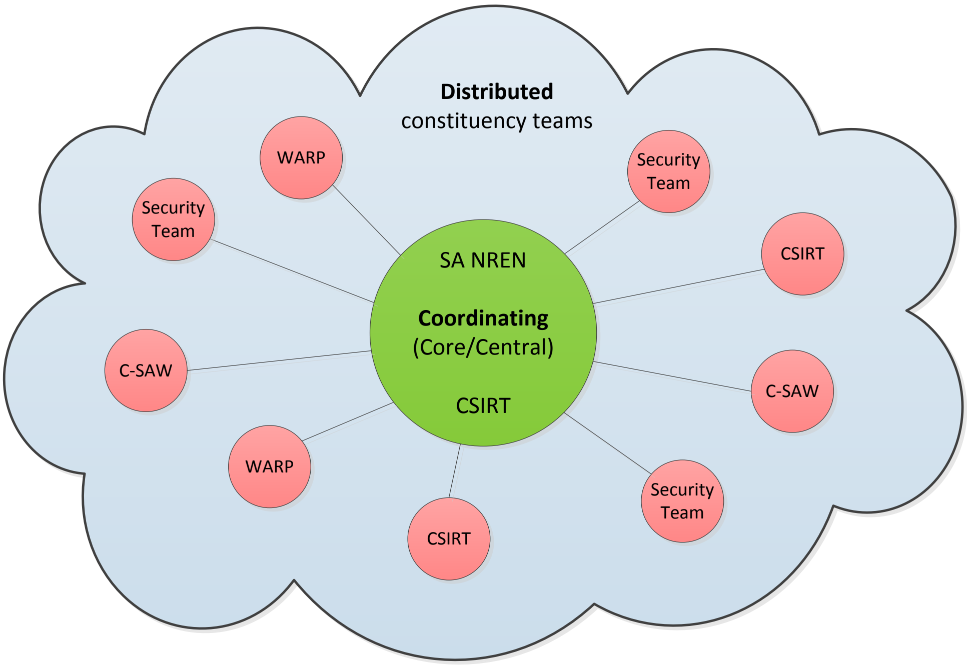


Figure 11.7: Team model for the SA NREN CSIRT (by author)

"As the coordinating CSIRT is most likely a dedicated team, it has a central location and manager" (Killcrece et al., 2003a, p. 115). The team model for the SA NREN comprises a combination of a core, central, *coordinating* CSIRT supporting *distributed* constituency teams. This model enables the efficient use of resources and facilitates participation of the constituency in CSIRT activities. It also adds structure to the existing teams within the constituency through coordination, with minimal disruption.

The coordinating team can be embedded within the SANReN and/or TENET organisations and therefore physically located in one of three possible locations — the CSIR in Pretoria (SANReN CA), the University of the Witwatersrand (WITS) in Johannesburg (TENET NOC) or the TENET head office in Cape Town. Although it has been advised that the team should be located in one central, physical location, some of the team members may participate virtually (following the distributed model format as per section 4.1, page 45). This allows a CSIRT team based at the CSIR in Pretoria to have distributed members from TENET and the constituency if required.

Determining staff requirements is partly dependent on the services selection and partners; therefore those areas are explored next.

11.2.2 Services (part i)

According to the CSIRT model, services are developed in parallel with people, processes, and tools and technologies due to the inputs and outputs to/from those respective areas. The constituency and funding have been considered and therefore the first part of selecting the services to be provided by the CSIRT is tackled here (as per section 9.2, page 133).

From the environment, the SA NREN CSIRT was shown to be an academic sector CSIRT serving the research and education institutions of South Africa in a coordinating role. In order to select the services, two primary sources of information can be consulted. Firstly, the core services for a coordinating CSIRT (as prescribed by Killcrece et al. (2003a)), and secondly, the results of the survey from chapter 10 highlighting the services that would be most useful to (and needed by) the constituency. Refer to table 3.2 (page 35) for the available options.

The basic services most often provided by coordinating CSIRTs, as argued by Killcrece et al. (2003a, pp. 117–120), are grouped under the applicable CSIRT service categories in table 11.2.

Considering that one of the incident handling services must be offered in order to be considered a CSIRT (section 6.1.1, page 79), the *incident response support and coordination* services make the most sense for the SA NREN CSIRT.

Table 11.2: Core services for coordinating CSIRTs (Killcrece et al., 2003a, pp. 117–120)

Reactive services	Alerts and warnings	
	Incident handling	Incident analysis Incident response support Incident response coordination
	Vulnerability handling	Vulnerability response coordination
	Artefact handling	Artefact response coordination
Proactive services	Announcements	
	Security-related information dissemination	
Security quality management services	Awareness building	
	Education and training	

Furthermore, from the survey, the most useful services were identified as (figure 10.6, page 159)

- alerts and warnings,
- training,
- security education, and
- security consulting (or recommendations).

Additional insights from the survey results (section 10.3.3) indicate that

a. training is indeed needed; this is confirmed by the fact that only 41% of staff from the institutions which responded to the survey have formal IT security training (figure 10.2b, page 155).

b. a coordination role would be more useful than offering direct incident handling services (incident handling is the third least useful service to respondents).

c. intrusion detection and incident response on site services should have low priority (as the least useful services to the constituency).

d. the top three services can be complemented by (or easily extended to include) security-related information dissemination.

Combining these with the previous table results in the following suggested initial services offering (portfolio) for the SA NREN CSIRT (proportionate to available funding):

- Reactive services
  - alerts and warnings, and
  - incident response support and coordination.
- Proactive services
  - announcements, and
  - security-related information dissemination.
- Security quality management services
  - awareness building, and
  - education and training.

These are shown in table 11.3. As the CSIRT matures and resources allow, the services portfolio can be expanded to include the next most useful services to the constituency (i.e. security consulting, vulnerability reporting and security audits/assessments). Note that security consulting was excluded from the initial set as it is not a typical coordinating CSIRT service; it would also require substantially more resources to provision.

Table 11.3: Initial services for the SA NREN coordinating CSIRT

Reactive services	Alerts and warnings Incident response support & coordination
Proactive services	Announcements Security-related information dissemination
Security quality management services	Awareness building Education and training

These services will further help the constituency recognise and deal with the incidents affecting them.

11.2.3 Partners (part i)

TENET internal partners include the network operations centre (NOC) staff as well as the 24x7 help desk who can be solicited as the first line support for computer security matters for the SA NREN CSIRT constituency. Clearly, policies and processes will need to be in place to support this.

Being part of the CSIR means that the SANReN CA team has access to various shared services[3], including

- Environment, Health and Safety (EHS) management;
- facilities management;
- finances;
- general support;
- Human Resources (HR);
- ICT;
- information and library;
- procurement;
- quality management;
- security; and
- stakeholder engagement (communications).

These internal partners can greatly assist the core team to establish a CSIRT for the SA NREN by providing advice and resources as detailed in section 7.1 (page 94). In addition, the CSIR provides internal audit as well as legal services which may be consulted with as required by the CSIRT.

Additionally, there are two competency areas (besides SANReN) within the CSIR performing information security related research. These are the Command, Control and Information Warfare (CCIW)[4] and the Modelling and Digital Science (MDS) information security[5] competency areas. Both groups can provide expertise (as listed on their respective web pages) which the SA NREN CSIRT can call upon if required.

These groups, together with the shared services partners, should be able to assist in establishing contact with external partners such as security experts, the media, law enforcement, coordination centres (e.g. the national CSIRT), service providers, etc. (see section 7.2, page 98).

[3] the list was obtained from an internal CSIR survey run in September 2014 accessed at `http://captiveportal.csir.co.za/limesurvey/index.php?sid=46547&lang=en*`

[4] `http://defsec.csir.co.za/?page_id=1993`

[5] `http://www.csir.co.za/MDS/Information_security.html`

Relationships with external partners, particularly other CSIRTs, should be explored through forums such as FIRST and Trusted Introducer (TI) (section 1.3, page 7). Considering that this CSIRT is for an NREN, registering with TI (which was established by the Trans-European Research and Education Networking Association (TERENA)) is the logical first step towards networking with external CSIRTs. Finally, having access to security experts from the constituency (being of a research and academic nature) is invaluable. Besides the CSIR, the universities in table 11.4 are known to have research groups focusing on areas of information security[6]. Networking with these researchers can provide valuable resources to supplement the SA NREN CSIRT staff and expertise. Furthermore, experts can be sought from the existing security teams of the constituency IT departments (see section 10.3.1, page 155).

11.2.4 SA NREN CSIRT Staffing considerations

Work schedule

Both the TENET and SANReN CA teams operate during *normal office hours* although members may be available after hours for emergencies. In the beginning of this chapter we further noted that TENET have outsourced a 24x7 help desk service. Considering the above, for the SA NREN CSIRT, it is recommended that services are offered during office hours (i.e. 9:00-17:00 on weekdays). Due to the potential ramifications of an IT security incident, the following approach is suggested:

1. Equip the 24x7 help desk staff to respond to basic incidents after hours. Depending on the severity of the incident, processes to guide the staff through first response should suffice (in the majority of cases) to reduce incident impact. Complete response can then resume during the next business day.

2. An escalation mechanism should be put in place so that the help desk can contact an incident handler for assistance if needed after hours. Incident severity and prioritisation (policies and processes) will dictate this. This essentially means that one of the CSIRT technical staff members needs to be on standby after hours.

[6] this information was partly derived from `http://www.infosecsa.co.za/Review_Panel`

Table 11.4: South African universities with information security research groups (by author)

University	Information Security Research Areas	Website
Nelson Mandela Metropolitan University	Management and governance (including standards, education and awareness)	http://iicta.nmmu.ac.za/Information-Security-Management-and-Governance
University of Fort Hare	Management and digital forensics	http://www.researchgate.net/profile/Stephen_Flowerday
University of Johannesburg	Governance + various (including policy specification and negotiation)	http://www.uj.ac.za/EN/Faculties/science/departments/csweb/research/Pages/default.aspx
University of South Africa	Various (including awareness and education)	http://www.unisa.ac.za/default.asp?Cmd=ViewContent&ContentID=23301#a3
University of Pretoria	Various (including digital forensics, privacy, vulnerability scanning and intrusion detection)	http://icsa.cs.up.ac.za/
Rhodes University	Computer networks	http://www.ru.ac.za/computerscience/researchgroups/securitynetworks/

This balance ensures that a 24x7 response will be possible for critical incidents without the need for a 24x7-staffed CSIRT.

Full- or part-time staff

Considering the choice of an embedded, central CSIRT supporting a distributed network of constituency security teams, having *full-time staff in the core* is the logical staffing model. This allows the coordinating team to be dedicated to incident handling activities without a conflict of interest from other responsibilities (section 4.1.1, page 46).

The *distributed teams* will most likely consist of *part-time staff* with other responsibilities. This allows for efficient resource utilisation and focus on incident handling activities only when required; though it must be communicated to and supported by their management. Additionally, it is important that a site security contact is reachable at all times so that the coordinating CSIRT can request information or response actions as required.

Staff numbers

Under *work schedule*, a weekdays 9:00-17:00 service offering was recommended for the coordinating CSIRT, with staff on standby after hours. Considering the as yet unknown workload, the ENISA advice of four full time equivalents is therefore advised for the coordinating CSIRT. That is, *four full-time staff members* for basic incident handling and advisory distribution (see section 4.1.1, page 46). This core team can execute the tasks necessary to implement the CSIRT and fill the required roles for operations (refer to section 11.2.4). Considering the access to a wide range of internal partners (section 11.2.3) this small team should be sufficient. Furthermore, the existing TENET NOC staff can be used as the first response help desk, reducing the load on incident handling staff. Additional staff can be employed (if required) once the CSIRT is handed over to TENET for operations.

Required staff skills

For the SA NREN CSIRT, the general technical skills from section 4.3.1 (i.e. *systems, networks, security, programming* and *internet*) are applicable. As mentioned in section 9.3.1 (page 135), specialised skills will depend on the selected services and the technologies in use by the constituency. From the initial services selection in table 11.3, it can be seen that the SA NREN will initially not be providing analysis, intrusion detection, security auditing or risk analysis services. This means that the specialised skills of malware analysis, forensics, intrusion detection, risk assessment and encryption (section 4.3.1, page 55) are probably not required. If necessary, partners can be used to fill knowledge gaps if necessary.

Considering the nature of the constituency, it is expected that a broad range of technologies is used. The most useful services to the constituency have already been included in the services selection. Furthermore, because there are skilled experts from the constituency in specialised areas (e.g. digital forensics) (see table 11.4) it is assumed that they can be utilised if required.

Thus, the required technical skills for the SA NREN coordinating CSIRT staff are the first five from table 4.3 (page 56). These are

1. systems,
2. networks,
3. security,
4. programming, and
5. the Internet.

Lastly, the personal skills from section 4.3.2 (page 56) should be included in job descriptions and interview questions as applicable for the SA NREN CSIRT staff.

Roles and responsibilities

Section 9.3.1 (page 135) states that roles and responsibilities depend on the environment, constituency and selected services. The staffing decisions already made in this section are also applicable. The most relevant ones are

a. staff numbers — four full-time staff, and

b. first response — being provided by the TENET NOC and/or help desk.

These lead to the following roles for the SA NREN coordinating CSIRT (based on section 4.2, page 48):

- *one team manager*, and
- *three incident handlers*.

A dedicated assistant manager is not required. As the team is small, it is assumed that the team manager will be highly available and a senior incident handler can always act as the proxy team manager if required.

The incident handlers will perform the actual delivery of services and are thus a crucial role for the SA NREN CSIRT. System and network administrators will be provided by the existing SANReN CA and TENET teams on a part-time basis. The first responder role will be filled by the TENET NOC and help desk (as explained in section 11.2.3). Lastly, considering the services portfolio, specialist vulnerability and artefact analysts are not required.

The extended team will be made up of people from the SANReN CA, TENET and partners as already discussed. This includes administrative roles which can be shared with the CSIRT.

11.2.5 Effects on the other requirements areas

In this section, the team model and staffing requirements for the SA NREN CSIRT were uncovered. These were done in parallel with the definition of services and partners. The links between these three areas as shown in figure 11.8 are:

- Services and Staff — the initial services selection provided input for the staff numbers and required skills. In implementation, these decisions will influence the depth of services that can be provided (e.g. number of announcements, frequency of education and training workshops, etc.).
- Staff and Partners — the primary partners for the SA NREN CSIRT were identified and elaborated on. These partners (including their accessibility and skills) guided the staffing decisions.

As shown in figure 11.8, staff identify and develop policies and processes as well as tools and technologies. These areas will be explored in the following sections.

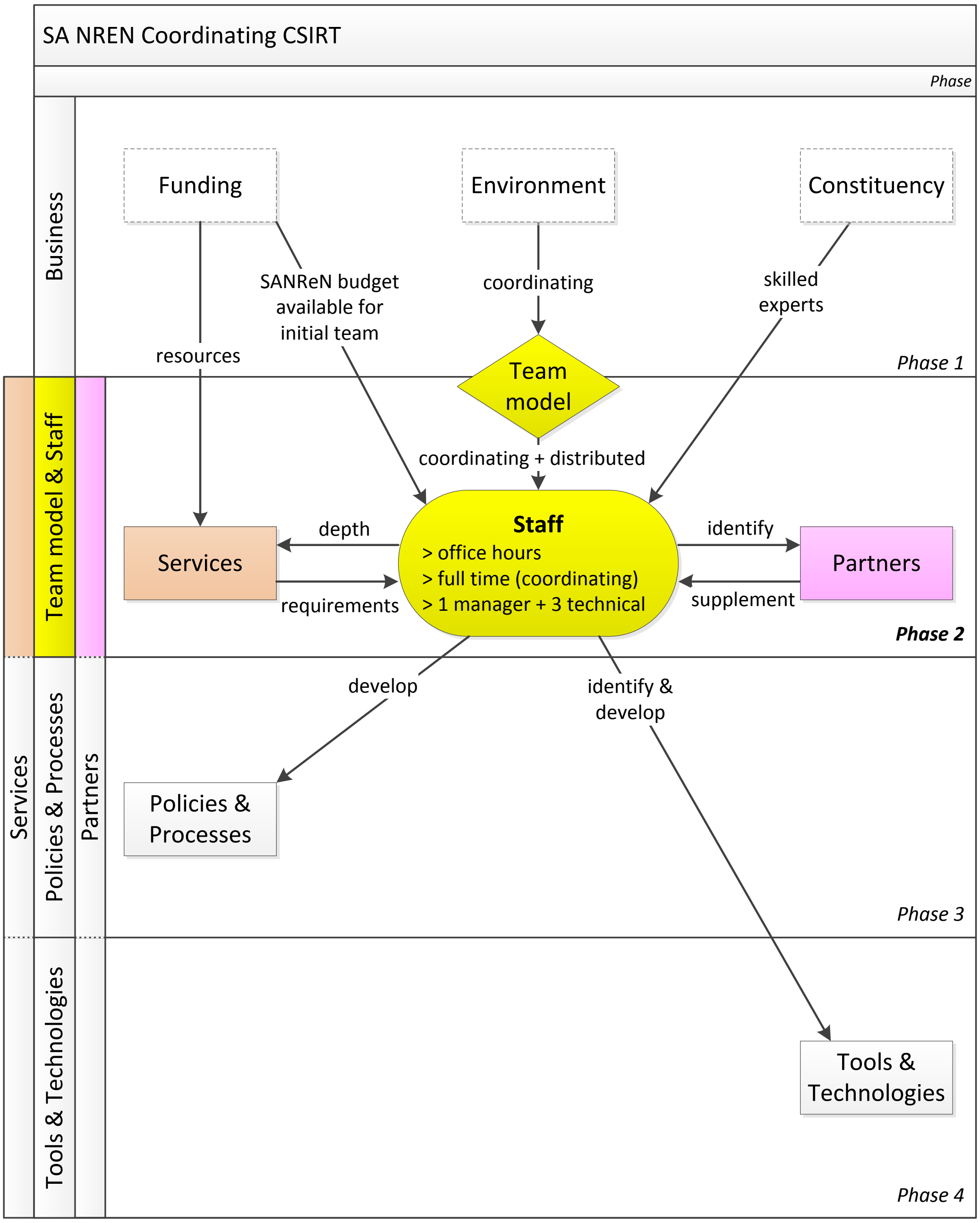


Figure 11.8: SA NREN CSIRT: People with links to other areas

11.3 Phase 3: Policies and Processes

Phase 3 of establishing a CSIRT is the design of the required policies and processes (section 9.3.2, page 138). This phase is shown in figure 11.9 and includes the continued parallel development of services and partners. The aim of this section is to reveal the policies and processes that need to be developed for the SA NREN CSIRT as well as their relationships to the other requirements. Following the breakdown used in chapter 5, the subsequent subsections address policies and processes in order. These are followed by the next round of services and partner developments, which are then brought together with the preceding decisions for policies and processes, showing the combined effect on the rest of the requirement areas.

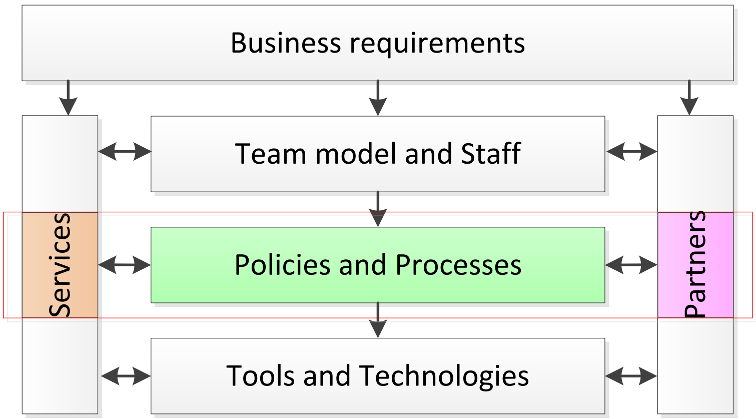


Figure 11.9: Phase 3: Policies and Processes for the SA NREN CSIRT

11.3.1 Inputs from the environment, services and staffing

Section 11.1.1 re-iterated that the CSIRT *mission and goals* provide a foundation for the policies and processes. The required policies and processes are additionally based on the *services* specified for the SA NREN CSIRT (section 11.2.2).

Therefore, policies and processes are required for

- mitigation of SANReN network and constituency incidents; and
- both reactive and proactive services, specifically
  - generating alerts and warnings,
  - incident response and coordination,
  - announcements,
  - security-related information dissemination,
  - awareness building, and
  - education and training.

Staff develop policies and processes (section 8.1, page 106); therefore the core team needs to be in place prior to actual development. Furthermore, the purpose of this section is to determine the required policies and processes for the SA NREN CSIRT and not to actually develop them.

11.3.2 SA NREN CSIRT policies

Policy development must occur in the context of the identified environment, i.e. as a coordinating CSIRT for a number of external organisations. The elements in table 5.1 (page 62) should additionally be integrated into each policy of the SA NREN CSIRT. For convenience, these are summarised in table 11.5. This integration can be achieved through the use of a policy template.

Table 11.5: Generic policy elements (from table 5.1)

Purpose and objectives
Management support statement
Scope and applicability
Relationships
Roles and responsibilities
Processes and procedures
Point of contact and policy maintenance
Glossary

Considering the inputs from the environment and services, the following policies are recommended for the SA NREN CSIRT:

- Fundamental policies (table 5.2, page 63) inclusive of
  - incident reporting and request handling (new policy),
  - data classification and prioritisation (new policy),
  - communications (with inputs from the CSIR policy),
  - information handling and disclosure (new policy),
  - media (based on the existing CSIR policy),
  - privacy (based on the existing TENET policy), and
  - security (based on CSIR policies).
- Secondary policies (section 5.1.3, page 66) inclusive of
  - service levels (based on the existing TENET agreement);
  - acceptable use (based on the existing TENET policy);
  - data, log and evidence retention (for compliance, legal and knowledge base (e.g. statistics) purposes);
  - code of conduct (based on the existing CSIR HR policies); and
  - human error (based on the existing CSIR HR policies).

These policies are indicated in table 11.6. The CSIR policies are not publicly available. The links to the existing TENET policies are:

- connection — `http://www.tenet.ac.za/doc/connection-policy`,
- acceptable use — `http://www.tenet.ac.za/doc/aup-3-2.pdf`,
- privacy — `http://www.tenet.ac.za/doc/privacypolicy.pdf`, and
- REN service agreement (service level indicators & targets) — `http://www.tenet.ac.za/doc/service-level-indicators-and-targets.pdf`.

The policies for the SA NREN CSIRT should be based on these existing policies, as far as possible, for consistency and to avoid duplication. Furthermore, information security policies from the constituency can provide inputs to these policies (68% of institutions have one (section 10.3.2, page 155)).

Table 11.6: SA NREN CSIRT policies (by author)

Policy	New/Based on existing
Incident reporting and request handling	New
Data classification and prioritisation	New
Communications	Based on existing (CSIR)
Information handling and disclosure	New
Media	Based on existing
Privacy	Based on existing (TENET)
Security	Based on existing (CSIR)
Service levels	Based on existing (TENET)
Acceptable use	Based on existing (TENET)
Data, log and evidence retention	New
Code of conduct	Based on existing (CSIR)
Human error	Based on existing (CSIR)

11.3.3 SA NREN CSIRT processes

The generic incident handling process from section 5.2.2 (page 67) is repeated for easy reference in figure 11.10. This process can be used "as is" for the SA NREN CSIRT noting that for the *respond* phase, due to the coordinating nature of the CSIRT, containment will be limited to the authority of the CSIRT and the specific nature of the incident. It is more likely that the CSIRT will be providing technical assistance and coordinating response actions than directly executing the actions required to resolve incidents.

Recalling that the SA NREN CSIRT will be providing alerts and warnings, announcements and security-related information dissemination services (see table 11.3); the information distribution process for alerts, warnings and announcements (see figure 5.3 on page 72) is also applicable.

In section 5.2 (page 67) it was argued that processes implement policy statements. Additional processes should therefore be developed as needed in alignment with the policies from the previous section.

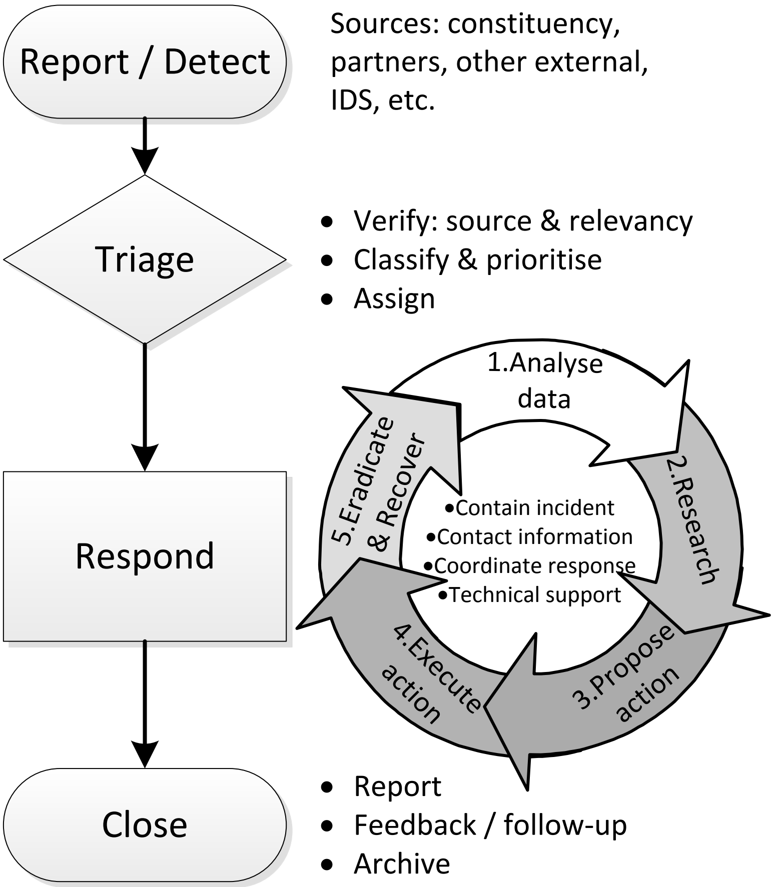


Figure 11.10: Generic incident handling process (from figure 5.1)

The applicable processes for the SA NREN CSIRT are subsequently identified from table 5.5 (page 74) as:

- information sharing,
- maintenance and tracking of data,
- public relations, and
- human resources.

These are combined with incident handling and information distribution in table 11.7 as a complete list of the processes for the SA NREN CSIRT.

Table 11.7: SA NREN CSIRT processes (by author)

Incident handling
Information distribution (for alerts, warnings and announcements)
Information sharing
Maintenance and tracking of data
Public relations
Human resources

Evidence preservation and forensics processes are not necessary for the initial phase of the CSIRT as neither the services, policies or identified staff skills support or require them. The references indicated in table 5.5 (page 74) can be consulted to determine to what extent the other processes are required and applicable.

11.3.4 Services (part ii)

In section 9.3.2 (page 139), it was shown that policies and processes describe services. Following the initial services selection (section 11.2.2), this section aims to develop the SA NREN CSIRT services further by highlighting the relevant inputs from the identified policies and processes.

To commence, the policies identified in section 11.3.2 are mapped to the appropriate SA NREN CSIRT services in table 11.8.

Table 11.8: SA NREN CSIRT policies to services mapping (by author)

Policy \ Service	Alerts and warnings	Incident response support & coordination	Announcements	Security-related information dissemination	Awareness building	Education and training
Incident reporting and request handling	✓	✓	✓			
Data classification and prioritisation	✓	✓	✓	✓		
Information handling and disclosure	✓	✓	✓	✓		
Privacy	✓	✓				
Service level agreements	✓	✓	✓			
Acceptable use	✓	✓	✓			
Data, log and evidence retention		✓				
Communications	✓	✓	✓	✓	✓	✓
Media	✓	✓	✓	✓	✓	✓
Security	✓	✓	✓	✓	✓	✓
Code of conduct	✓	✓	✓	✓	✓	✓
Human error	✓	✓	✓	✓	✓	✓

The predominant role of the incident handling service is re-enforced by the observation that all policies are somehow related to incident response support and coordination (as an incident handling service). Furthermore, the communications, media, security, code of conduct and human error policies are associated across all of the SA NREN CSIRT services. The *communications* policy because all services involve communications technologies, data exchange, key handling and/or notification in some form; the *media* policy because any service (whether distributing information or handling an incident) can result in interactions with the media. By dealing with physical, personnel and ICT security, the *security* policy affects all services (see section 5.1.2, page 61). The *code of conduct* and *human error* policies define and dictate staff behaviour and attitudes across all services.

The *incident reporting and request handling* policy has only been mapped to services which specifically deal with incidents and requests, that is the alerts and warnings, incident response support and coordination, and announcements services. Similarly, the *data classification and prioritisation* as well as *information handling and disclosure* policies are not applicable to the awareness building and education and training services as the "data" used in those services should be unclassified (or suitably sanitised) and do not typically warrant prioritisation. The *privacy* policy also does not apply to services where privacy is not required such as announcements or awareness building where any confidential information should be suitably sanitised instead.

Service level agreements are only really applicable to reactive services and perhaps announcements where a certain level of response (e.g. timeliness) is expected. The same services are related to acceptable use where infringement triggers response services and announcements can be made. Finally, *data, log and evidence retention* is arguably only applicable to the incident handling service as that is where data, logs and evidence are handled and retained (in a ticketing system database for example). Thereafter, the policy has already been applied when/if utilised by other services.

Next, the processes for the SA NREN (section 11.3.3) are mapped to the services as shown in table 11.9.

Table 11.9: SA NREN CSIRT processes to services mapping (by author)

Process / Service	Alerts and warnings	Incident response support & coordination	Announcements	Security-related information dissemination	Awareness building	Education and training
Incident handling	✓	✓	✓			
Information distribution	✓		✓			
Information sharing	✓	✓	✓	✓	✓	✓
Maintenance and tracking of data	✓	✓	✓	✓	✓	✓
Public relations	✓	✓	✓	✓	✓	✓
Human resources		✓				✓

The incident handling process details the steps followed for the incident response support and coordination service. This process may additionally trigger alerts, warnings and/or announcements. As described in section 5.2.3 (page 71), the information distribution process thus applies to these two services.

Due to the fact that information is shared across all processes (including the outputs from information distribution), the information sharing process applies to all services. The collection, use, archiving and tracking of data applies across the services. Interactions with the media can also occur for any service. Lastly, the process(es) for human resources apply to the incident response support and coordination service (in the context of staff extension) as well as to education and training (see section 5.2.4, page 73).

11.3.5 Partners (part ii)

Policies and processes should include cooperation agreements, service levels and reporting requirements for partners; partners can it turn assist with developing policies and processes (section 9.3.2, page 138).

Seven of the SA NREN CSIRT *policies* involve partners either as participants, providers or users. These are

1. incident reporting and request handling (as partners can report incidents or make requests);
2. data classification and prioritisation (of information received from partners);
3. communications (technologies, standards, notification, etc.);
4. information handling and disclosure;
5. media (applying to the media as an external partner);
6. privacy (extended to partners); and
7. service level agreements.

The acceptable use as well as the data, log and evidence retention policies are not enforceable on partners (except where partners form part of the constituency or CSIRT staff). To supplement this, a cooperation agreement with partners can be used, carrying over the required elements from these policies. The security, code of conduct and human error policies have minimal (if any) effect on partners because they address internal behaviour. When partners are seconded as CSIRT staff though, then these policies will apply.

Four of the SA NREN CSIRT *processes* (from table 11.7) similarly involve partners. These are

1. incident handling (with partners as a source and/or consultant),
2. information distribution (partners as a source or recipient),
3. information sharing (with partners), and
4. public relations (dealing with the media).

The processes for maintenance and tracking of data as well as human resources are internal to the CSIRT (only applying to partners if seconded as staff).

Partners, particularly other CSIRTs, can provide input to policies and processes (section 9.3.2, page 139). To benefit from this, the SA NREN CSIRT staff should establish contact and network with other NREN CSIRTs as early as possible. Section 11.2.3 suggested pursuing memberships with FIRST and TI as the preferred approach. In addition, the identified internal partners as well as SANReN and TENET staff can provide input to the CSIRT policies and processes. Lastly, the establishment team for the South African National CSIRT — the Cybersecurity Hub (Grobler et al., 2012) — may also be able to provide advice or templates for policies and processes.

11.3.6 Effects on the other requirement areas

In this section, the required policies and processes for the SA NREN CSIRT were discussed, together with the further development of services and partners. In summary:

- Services are based on Policies and Processes. To illustrate this, the mapping of services to policies as well as services to processes was shown in this section, highlighting which policies and processes will describe which services.
- Partners provide input to Policies and Processes. Partner interactions are also described by the relevant policies and processes (indicated in section 11.3.5).

To conclude this section, policies and processes guide the development of tools and technologies (as argued in section 9.3.2, page 139) which are discussed next. All of these links are shown in figure 11.11.

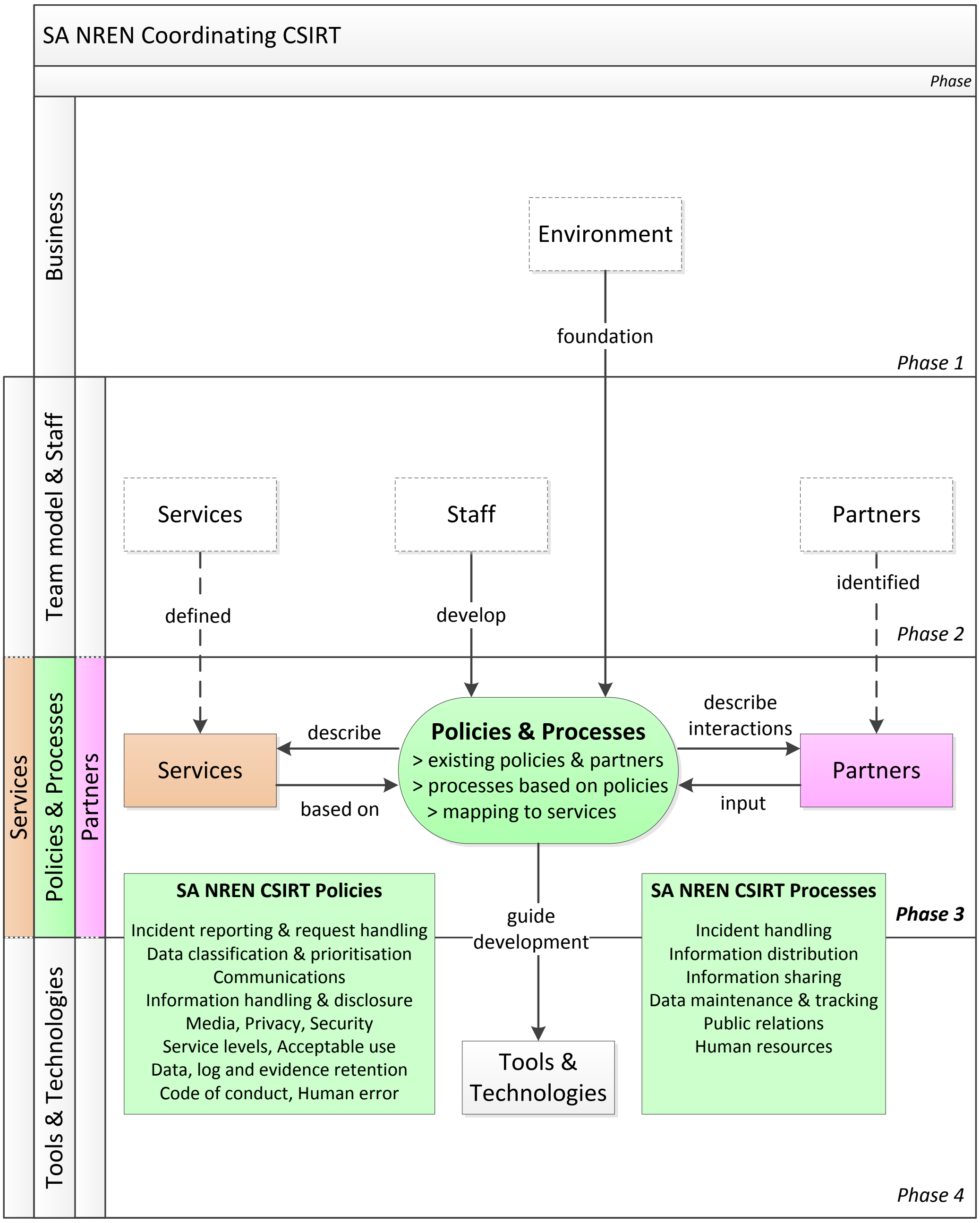


Figure 11.11: SA NREN CSIRT: Policies & Processes with links

11.4 Phase 4: Tools and Technologies

In section 9.3.1 (page 135) it was shown that people identify, develop and/or obtain tools and technologies for CSIRT operations. The fourth and final phase of the model proposed in this dissertation is the identification of the required tools and technologies. Considerations for services and partners will also be completed in this phase. This phase is shown in figure 11.12.

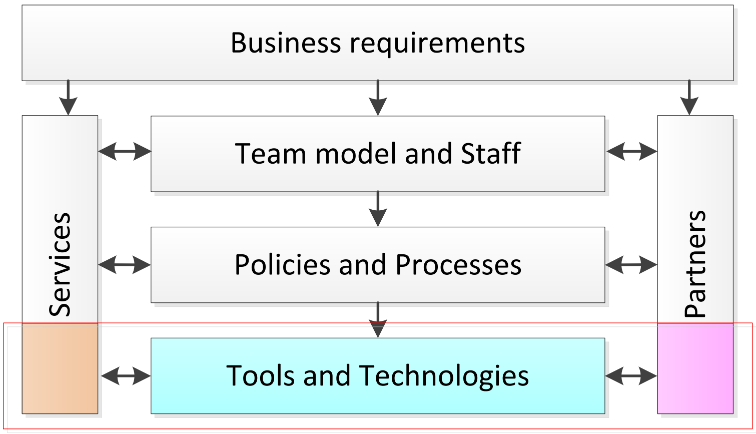


Figure 11.12: Phase 4: Tools and Technologies for the SA NREN CSIRT

11.4.1 Inputs from the other areas

From the business requirements (pages 131 and 132), it can be seen that

a. the needs of the *constituency* determine the required tools and technologies, and

b. *funding* influences the procurement and/or development of tools and technologies.

Sections 9.3.3 and 9.3.4 (pages 140 and 142) further summarise the links from the other Ps to tools and technologies as follows:

- *Staff* develop and/or obtain tools and technologies.
- *Policies and processes* guide the development of tools and technologies.
- The definition of *services* helps determine which tools and technologies are needed.
- *Partners* can address deficiencies in tools and technologies (supplementing them with their own resources). They can also recommend or provide tools and technologies to the CSIRT.

These relationships are illustrated in figure 11.13. This shows that determining the requirements for staffing, policies and processes as well as service definitions (as addressed in the preceding sections) are necessary prior to identifying the required tools and technologies. Additionally, tools and technologies are based on constituency needs as well as available funding.

The relevant SA NREN CSIRT decisions taken so far are covered in the rest of this section.

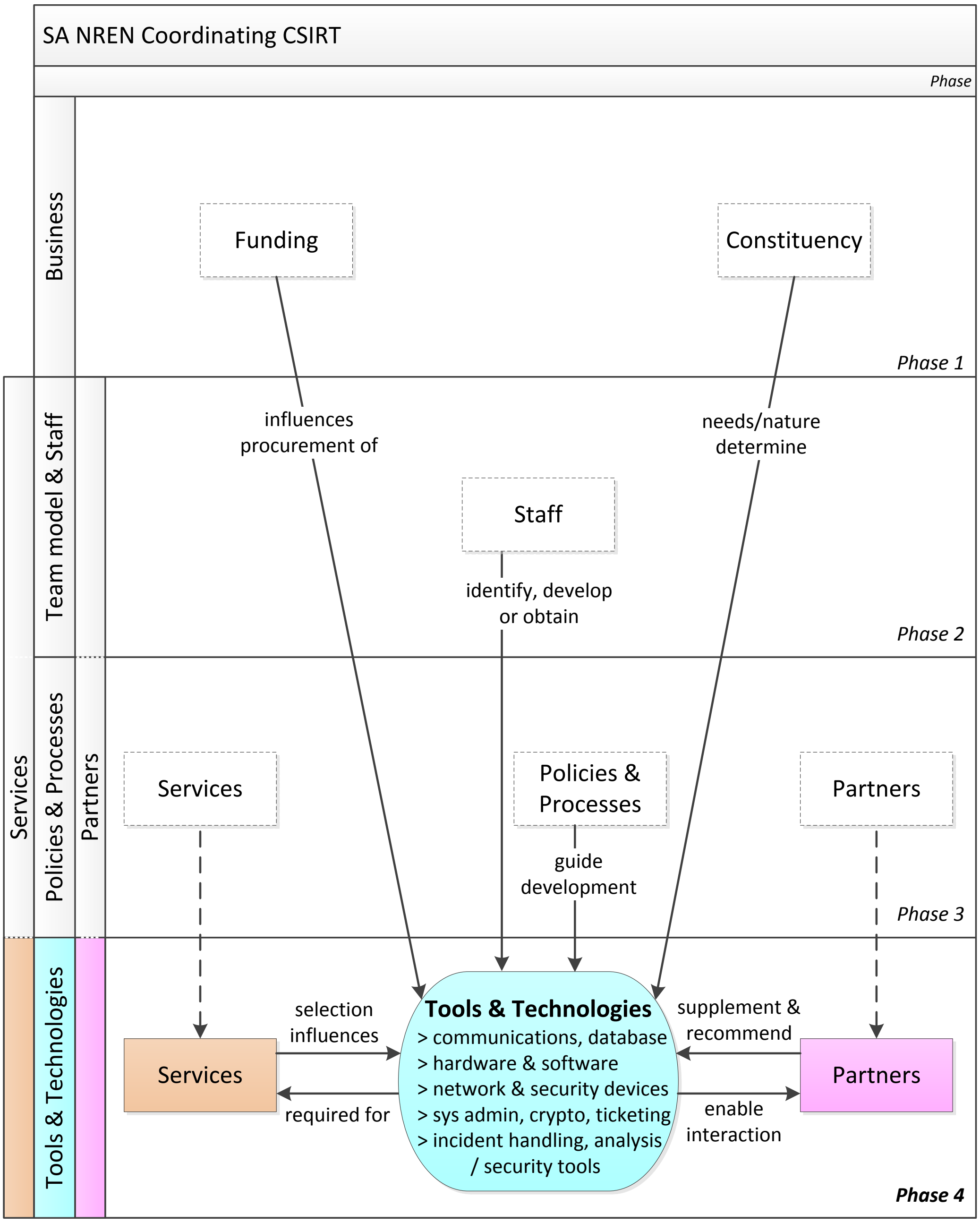


Figure 11.13: SA NREN CSIRT: Tools & Technologies with links

Constituency and funding

Being situated in the academic and research environment means that the constituency (the users and their ICT staff) should be using (or at least able to use) encryption/decryption tools. Equipping the constituency to use digital signatures and encryption for communicating electronically with the CSIRT should therefore be straightforward. The constituency additionally has high bandwidth, low latency links to the Internet. The SANReN network has been designed for redundancy; in addition, TENET warrant constant availability for the network[7] ensuring its reliability. This makes the use of web, email and other electronic communication mechanisms attractive options for the SA NREN CSIRT.

In order to minimise cost, existing open source tools and technologies should be used where possible. Partners can assist with recommendations in this regard. They can also advise on the most cost-effective solutions where hardware and software need to be purchased. Other CSIRTs may have tools and technologies which they have developed and are willing to share with the SA NREN CSIRT (at zero or minimal cost). Once the CSIRT is handed over to TENET, further procurement and/or development of tools and technologies will be influenced by the revised (and as yet undetermined) budget.

Finally, the SA NREN CSIRT can advise the constituency on suitable tools and technologies to combat the malicious activity affecting them (e.g. anti-malware, anti-spam, etc.).

Staffing

Both the number of staff as well as their skills affects the tools and technologies that can be used by the team. Development of tools requires time, effort and skills (e.g. programming). The roles identified for the SA NREN CSIRT (see section 11.2.4) *do not* leave room for the development of tools and technologies. If the required tools (identified in the next section) cannot be procured in a ready to use (or almost ready to use) form then additional staff with the required skills are needed. Furthermore, the use of some tools require unique skills, training or experience that may not be available in the team (e.g. advanced scanning tools, intrusion detection systems, etc.).

[7] `http://www.tenet.ac.za/doc/tenet-ren-service-agreement-redistributable`

Finally, the distributed nature of the constituency and the subsequent decision to establish the SA NREN CSIRT in a coordinating role mean that certain tools and technologies are more applicable than others (as clarified by the services requirements).

11.4.2 SA NREN CSIRT tools & technologies

Section 9.3.3 (page 140) shows the main tools and technologies that are required for a CSIRT (based on table 6.2, page 84). Each one is briefly discussed and applied to the SA NREN CSIRT in the following subsections. The recommendations are summarised in table 11.10.

Table 11.10: SA NREN CSIRT tools & technologies (by author)

Tool / Technology	SA NREN CSIRT proposal
Communications	Primarily Internet-based
Cryptographic	PGP (GnuPG)
Ticketing system	RTIR / OTRS
Incident handling, analysis or security	As needed
General hardware and software	Mostly already provided (add: smartphones, shredder, safe)
Network and security devices	Reuse existing
System administration	Reuse existing/supplement
Contacts database	Append existing SANReN/TENET database

Communication mechanisms

In section 11.4.1 it was argued that Internet-based communication mechanisms are good options for the SA NREN CSIRT. Both the SANReN and TENET teams use email as the primary form of communication. They likewise have websites and make use of mailing lists. Phones, fax and video conferencing facilities are available as alternatives. Email can easily be re-used by the CSIRT with the addition of encryption for sensitive data.

Cryptographic mechanisms

Pretty Good Privacy (PGP) emerged from section 6.2.2 (page 85) as the recommended cryptographic mechanism for CSIRTs. The GNU Privacy Guard (GnuPG)[8] is a complete and free implementation of the OpenPGP standard. It can be easily integrated into popular email clients for encryption and verification (signing) purposes. The SA NREN CSIRT would be able to use it with essentially no cost and minimal effort (creating, uploading and storing keys and configuring an email client to use them).

Ticketing system

SANReN currently use the Request Tracker (RT) ticketing system; TENET make use of Open Technology Real Services (OTRS). Section 6.2.3 (page 85) remarked that Request Tracker for Incident Response (RTIR) (based on RT) appeared to be the most popular amongst NRENs and is thus the logical option. Alternatively, OTRS can be used if preferred by the CSIRT and depending on where it will be hosted. The final choice can be made during implementation.

Incident handling, analysis or security tools

Section 6.2.4 (page 86) argued that many of the tools in this category are related to specific CSIRT services. Most of these tools can be obtained or developed as needed by consulting both the references in that section as well as partners (other CSIRTs, researchers, experts from the constituency, etc.). The primary initial tools that will be required by the SA NREN CSIRT include the network, incident handling and statistics/correlation tools from table 6.3 (page 88). During establishment, the specific tools required can be assessed and acquired by the team.

General hardware and software

Typically, hardware and software required for operations is provided by the CSIR (for the SANReN CA) and TENET for their respective staff. On the hardware side these include networking equipment, security appliances, servers, laptops, backup media, lab and test equipment as well as printers, scanners and fax machines.

[8] https://www.gnupg.org

The remaining hardware that needs to be considered for the SA NREN CSIRT are smartphones (staff use their personal phones at the moment), shredder(s) and a safe (from section 6.2.5, page 87). Although there are virtual servers available for CSIRT use, dedicated machines (with stricter security policies) should be considered. Standard software, including operating systems and office applications, is provided by the CSIR and TENET. Free and Open Source Software (FOSS) can be utilised for most other CSIRT purposes (e.g. Linux-based operating systems, tools/applications to secure remote access and security (see section 6.2.5, page 87)). Other software that may need to be purchased, in particular some of the specialised CSIRT tools, can be addressed on a case by case basis as the budget permits.

Network and security devices

This includes a mechanism to isolate the CSIRT network and machines from the Internet such as a firewall complemented with centralised logging and reporting (section 6.2.6, page 90). The most cost effective approach for the SA NREN CSIRT will be to reuse existing SANReN and TENET infrastructure providing recommendations for supplementing this where needed (e.g. hardening). This is reinforced by policies and processes for updating, patching and monitoring, etc. the devices. The added benefit is that the entire SANReN CA and TENET teams' operations are better protected. There are some disadvantages to this approach though including the possibility of human error, failed/delayed implementation of policies and processes or even malicious insiders. Addressing these require a well-managed implementation.

System administration tools

SANReN and TENET are already using these tools, so the CSIRT can simply reuse them where required. Where system administration tools are missing or incomplete, the CSIRT can make recommendations for improvement based on the team's needs, knowledge gained from CSIRT literature (e.g. section 6.2.7, page 90) and/or partner interactions.

Contacts database

Both the SANReN CA and TENET make use of a contacts database of some sort. Ideally the CSIRT should make use of these systems, supplementing the data with information for security contacts at the sites of the constituency.

The actual development or procurement of the tools and technologies mentioned in this section will occur during CSIRT establishment and operations. Other tools and technologies (see section 6.2.9, page 91) can be explored as the CSIRT gains practical experience revealing which will be useful.

11.4.3 Services (part iii)

The initial services selected for the SA NREN CSIRT are shown in table 11.3 (page 180). This was supplemented by showing the relationships between and mapping the SA NREN CSIRT policies and processes to these services (section 11.3.4). Section 9.3.3 (page 140) argued that tools and technologies are required for services. It further notes that *services definitions are required to know which tools and technologies are needed* (page 141). These associations are shown in figure 11.14. This section continues the development of services for the SA NREN CSIRT by mapping the identified tools and technologies to the selected services in table 11.11.

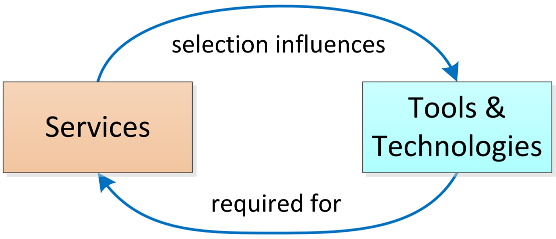


Figure 11.14: Relationship between Services and Tools & Technologies

The technologies and tools are ordered by the number of services that depend on or utilise them. As seen in the table, communications technology, the contacts database and general hardware and software are required by all services. Network and security devices are mainly applicable to the incident response support and coordination service, but do indirectly affect the other services as data passes through the devices. Administration tools do not add directly to the provision of services though they do contribute to the maintenance of the systems that help provision them (hence the "half-ticks"). Note additionally that providing education and training services do not require network and security devices or system administration tools as the service can be provisioned using a desktop/laptop with reporting writing and/or presentation software (no special servers or networks are required).

Table 11.11: SA NREN CSIRT tools & technologies to services mapping (by author)

Service Tool / Technology	Alerts and warnings	Incident response support & coordination	Announcements	Security-related information dissemination	Awareness building	Education and training
Communications	✓	✓	✓	✓	✓	✓
Contacts database	✓	✓	✓	✓	✓	✓
General hardware and software	✓	✓	✓	✓	✓	✓
Network and security devices	✓^	✓	✓^	✓^	✓^	
System administration	✓^	✓^	✓^	✓^	✓^	
Cryptographic	✓^	✓	✓^	?		
Ticketing system	?	✓	?			
Incident handling, analysis or security		✓				

✓= applies
✓^= applies indirectly or in certain circumstances
? = implementation dependent

Cryptographic technology is used primarily to protect sensitive communications for incident response and coordination. It can also be used to verify the origin of information provided by the CSIRT, through the use of digital signatures, for the indicated services. Cryptography is not generally used for awareness building or education and training as that information is not sensitive and/or should be sanitised instead prior to publication or presentation. This could additionally apply to the dissemination of security-related information. The ticketing system and incident handling, analysis and security tools are only really used for incident response support and coordination. Ticket numbers may be assigned to alerts and announcements though for tracking purposes (West-Brown et al., 2003, p. 99). This mapping confirms that the identified tools and technologies are required by the services selected for the SA NREN CSIRT.

11.4.4 Partners (part iii)

Tools and technologies enable coordination of partners as well as interactions with them. Partners can in turn supplement the required tools and technologies (section 9.3.4, page 142). This subsection investigates this relationship for the SA NREN CSIRT (shown in figure 11.15).

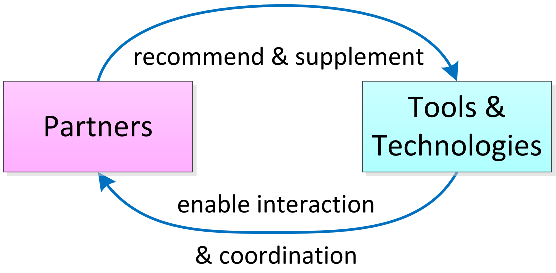


Figure 11.15: Relationship between Partners and Tools & Technologies

Firstly, it should be clear that the tools and technologies in table 11.10 facilitate partner interactions: from the database providing contact details, to the laptop used for typing an email and the communications technology used to deliver it. Cryptography is also used where applicable and the ticketing system stores relevant information and reports from partners.

As for policies and processes, other CSIRTs, and even the cybersecurity hub (Grobler et al., 2012), could suggest and possibly provide some of the required tools and technologies. CSIR internal partners and other security research groups can further assist with recommendations and provision of the required tools and technologies (see section 11.2.3, page 180).

Finally, as a specific example, PGP is based on a web of trust: user A (already trusted by a community) can the sign the key of user B to verify that the key belongs to user B. PGP utilises this concept to form groups of "introducers" and ultimately a "web of trust"[9]. Partners from TI and FIRST can act as introducers for the SA NREN CSIRT thereby accelerating the process of gaining the trust of the CSIRT community.

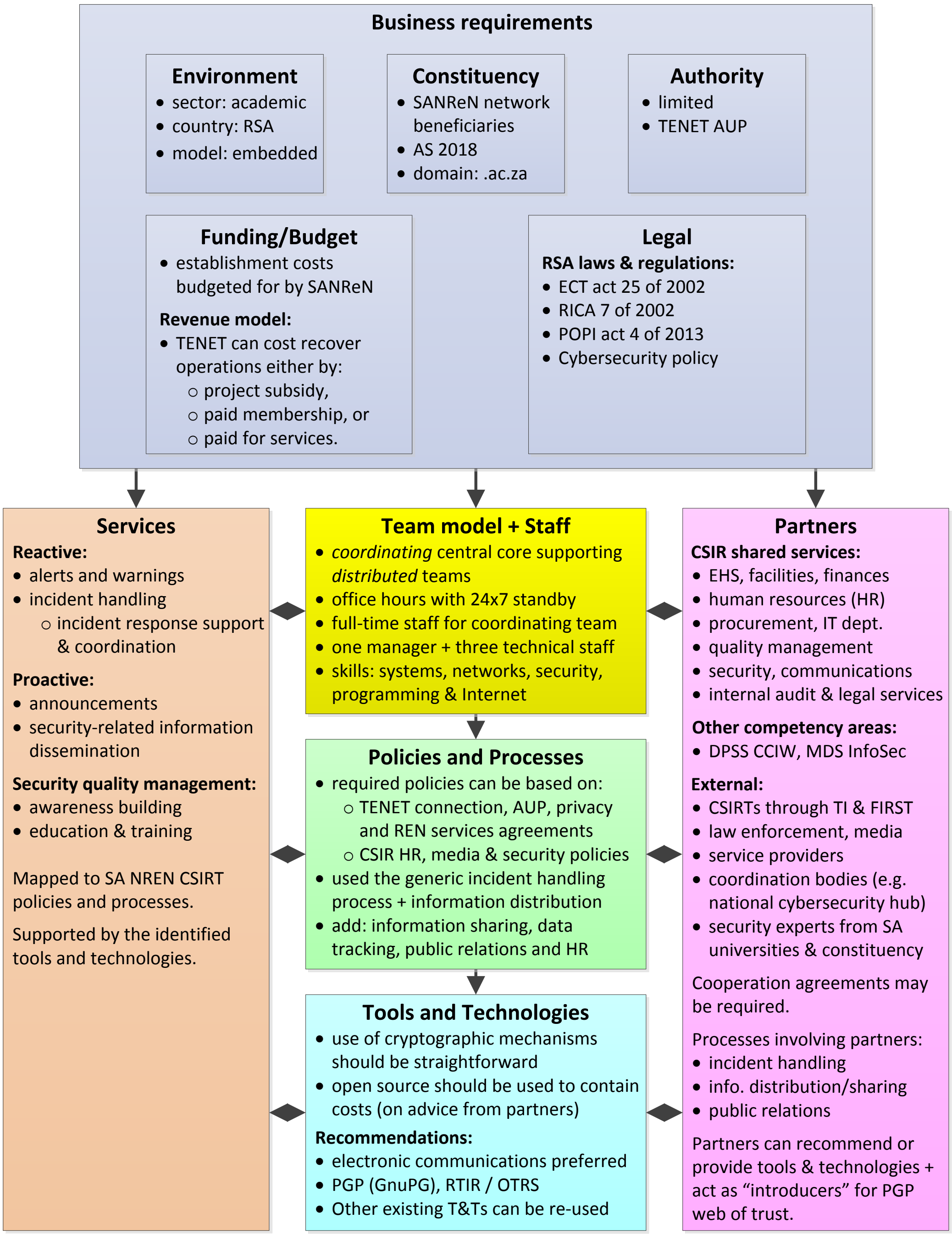
11.5 Summary of the model for the SA NREN CSIRT

Figure 11.16 presents a summary of the findings and recommendations of this chapter.

The development of the model of a CSIRT for the SA NREN commenced by addressing the business requirements (section 11.1). This was achieved through an exploration of the SA NREN environment, providing a basis for the subsequent decisions. The CSIRT was classified as an *academic sector* CSIRT as it serves an NREN constituency covering the whole of the *Republic of South Africa*. Applicable *laws and regulations of the RSA* were subsequently identified. Two possible hosting organisations for the CSIRT were uncovered, namely, the CSIR (host of the SANReN CA) and TENET. This indicated that an *embedded organisational model* would be the best approach. Following the specification of the environment, a mission was defined for the CSIRT as input to the constituency, services, and policies and processes.

The constituency was defined as the *SANReN network beneficiaries* and part of *Autonomous System (AS) 2018* — the TENET AS. This revealed the *limited authority* the CSIRT would have over the constituency, primarily enforceable through an AUP. The initial funding would be provided by SANReN, with subsequent operational funding provided by TENET using one of three possible approaches.

[9] `http://www.pgpi.org/doc/pgpintro/`



Business requirements

Environment
- sector: academic
- country: RSA
- model: embedded

Constituency
- SANReN network beneficiaries
- AS 2018
- domain: .ac.za

Authority
- limited
- TENET AUP

Funding/Budget
- establishment costs budgeted for by SANReN

Revenue model:
- TENET can cost recover operations either by:
  - project subsidy,
  - paid membership, or
  - paid for services.

Legal

RSA laws & regulations:
- ECT act 25 of 2002
- RICA 7 of 2002
- POPI act 4 of 2013
- Cybersecurity policy

Services

Reactive:
- alerts and warnings
- incident handling
  - incident response support & coordination

Proactive:
- announcements
- security-related information dissemination

Security quality management:
- awareness building
- education & training

Mapped to SA NREN CSIRT policies and processes.

Supported by the identified tools and technologies.

Team model + Staff
- *coordinating* central core supporting *distributed* teams
- office hours with 24x7 standby
- full-time staff for coordinating team
- one manager + three technical staff
- skills: systems, networks, security, programming & Internet

Policies and Processes
- required policies can be based on:
  - TENET connection, AUP, privacy and REN services agreements
  - CSIR HR, media & security policies
- used the generic incident handling process + information distribution
- add: information sharing, data tracking, public relations and HR

Tools and Technologies
- use of cryptographic mechanisms should be straightforward
- open source should be used to contain costs (on advice from partners)

Recommendations:
- electronic communications preferred
- PGP (GnuPG), RTIR / OTRS
- Other existing T&Ts can be re-used

Partners

CSIR shared services:
- EHS, facilities, finances
- human resources (HR)
- procurement, IT dept.
- quality management
- security, communications
- internal audit & legal services

Other competency areas:
- DPSS CCIW, MDS InfoSec

External:
- CSIRTs through TI & FIRST
- law enforcement, media
- service providers
- coordination bodies (e.g. national cybersecurity hub)
- security experts from SA universities & constituency

Cooperation agreements may be required.

Processes involving partners:
- incident handling
- info. distribution/sharing
- public relations

Partners can recommend or provide tools & technologies + act as "introducers" for PGP web of trust.

Figure 11.16: Summary framework of the SA NREN CSIRT model (by author)

The CSIRT team model and staffing requirements were examined next (section 11.2). This included the decision to utilise a central *coordinating* CSIRT model supporting *distributed* constituency teams as appropriate for the environment. An *office hours* work schedule was proposed with 24x7 support from the TENET help desk with CSIRT staff on standby for escalation.

An initial staff complement of *four full-time* members — one manager and three technical staff (incident handlers) — was advised, following recommendations from literature. *Systems, networks, security, programming and Internet skills* were deemed sufficient for these staff members. First response should be provided by the TENET NOC and/or help desk to support these low staff numbers. Other SANReN and TENET staff as well as internal partners will comprise an extended team to further support the CSIRT.

In parallel with addressing the team model and staff requirements, initial services (section 11.2.2) and partners (section 11.2.3) were identified. *Six initial service offerings* were selected for the CSIRT. These are

1. alerts and warnings,
2. incident response support and coordination,
3. announcements,
4. security-related information dissemination,
5. awareness building, and
6. education and training.

Additional services can be added later in line with constituency requirements and resource availability.

Internal partners were identified from *CSIR shared services* and other *competency areas performing information security research* in the CSIR. Registering with TI was recommended as a first step towards networking with *other CSIRTs.* In addition, *security experts* from the universities and IT departments of the constituents could be valuable external partners. The national CSIRT (*Cybersecurity Hub of South Africa*) was recognised as a potential coordination centre. Other external partners, whom the CSIRT should establish relationships with, include *law enforcement, the media and service providers.* These services and partners were mapped to the SA NREN CSIRT policies and processes, and tools and technologies, in the subsequent phases of development.

The next phase determined the required policies and processes (see section 11.3). Following the recommendation to make use of a *policy template*, the policies required for the SA NREN CSIRT were identified. These are shown in table 11.6. The SA NREN CSIRT processes include the *generic incident handling process* as well as the *process for information distribution*. Additional processes were suggested as shown in table 11.7. Besides the mapping showing the relevant policies and processes for each service (section 11.3.4), the policies and processes affecting and involving partners (section 11.3.5) were revealed as further development in those two areas.

The final phase advised on the required tools and technologies for the SA NREN CSIRT, providing suggestions for implementation where applicable (section 11.4). These recommendations include the use of electronic communications coupled with cryptographic mechanisms for securing communications. Open source solutions should be sought where practicable, on the advice of partners, in order to contain costs. GnuPG was recognised as a good solution for PGP implementation; with RTIR (based on RT used by the SANReN CA) or OTRS (currently used by TENET) for a ticketing system.

In this final phase of development, it was observed that services are supported by these tools and technologies (section 11.4.3). Lastly, partners can recommend or provide tools and technologies; they can also act as introducers to the rest of the security community via the PGP web of trust (section 11.4.4).

This concludes the model for the SA NREN CSIRT demonstrating the effective utility of the generic model for establishing a CSIRT.

11.6 Conclusion

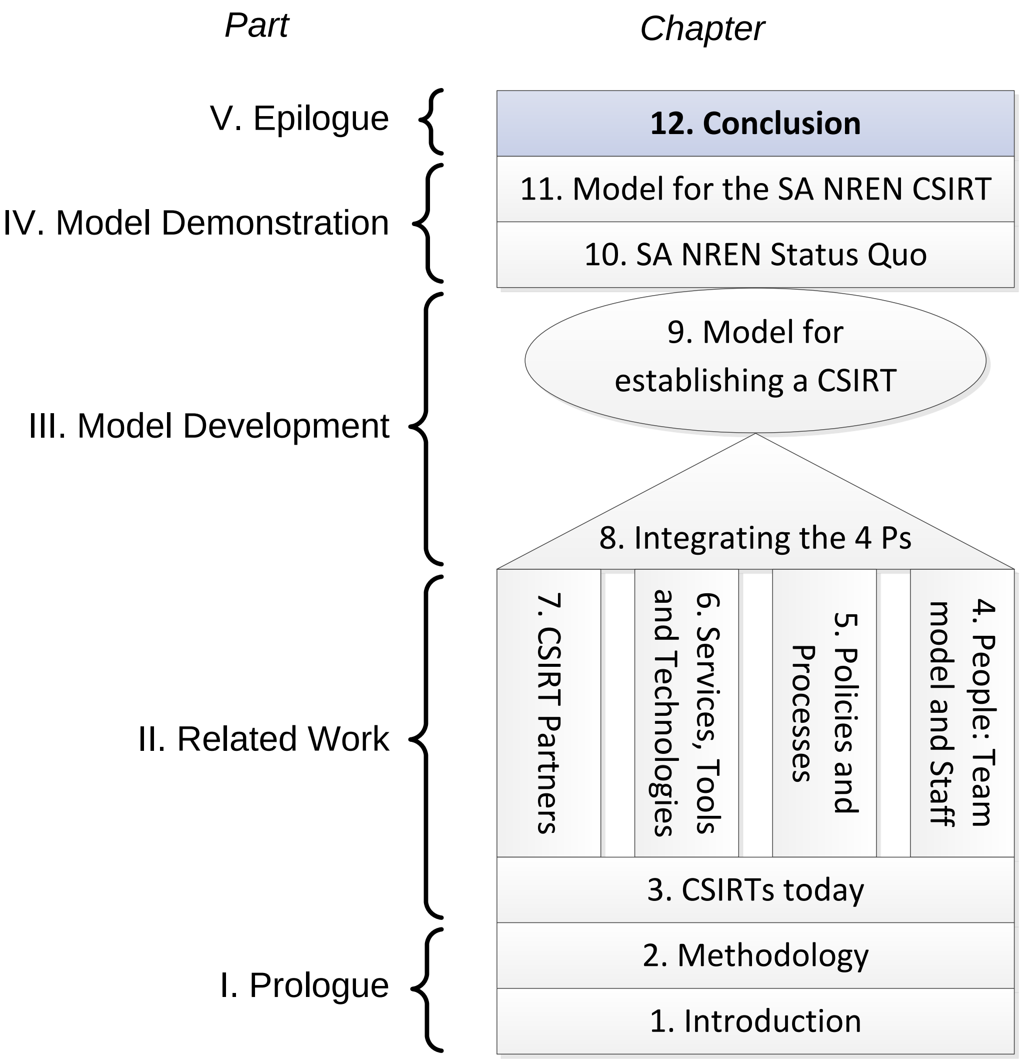
This chapter applied the generic model for establishing a CSIRT to design a specific model for the SA NREN CSIRT. Each of the phases was explored to determine the business requirements and subsequently people, policies and processes, and tools and technologies in turn. Services and partners were developed in parallel, following the generic model.

The model was successfully applied to the SA NREN environment as all phases could be addressed completely and in order. Actual implementation of this model, i.e. establishing the CSIRT, is beyond the scope of this dissertation, but is the logical next step for this research.

The next chapter concludes this dissertation by summarising the objectives of this research and the work done in achieving those objectives. The results will be discussed and areas for future research proposed.

Part V

Epilogue


Part
Chapter
V. Epilogue
12. Conclusion
IV. Model Demonstration
11. Model for the SA NREN CSIRT
10. SA NREN Status Quo
III. Model Development
9. Model for establishing a CSIRT
8. Integrating the 4 Ps
II. Related Work
7. CSIRT Partners
6. Services, Tools and Technologies
5. Policies and Processes
4. People: Team model and Staff
3. CSIRTs today
I. Prologue
2. Methodology
1. Introduction

Chapter 12

Conclusion

The previous chapter completed the demonstration part of this dissertation by applying the model for establishing a CSIRT in the SA NREN environment. Each phase of the model framework was addressed in turn, answering the questions and making the decisions along the way for the design of the SA NREN CSIRT. This ranged from the business requirements through to the required tools and technologies, while services and partners were developed as progression was made through the other Ps. The specific model was successfully completed, demonstrating the utility of the generic CSIRT model.

This chapter concludes the research by arguing that successful design science artefacts have been developed and demonstrated to solve the problems initially presented in chapter 1. First off, the problem statement and research objectives are revisited before highlighting the key findings of this study. The methodology used is discussed next, followed by a summary of the conclusions presented for each chapter of the dissertation. After this, the research contributions, based on the DSR framework are described. The final section discusses the limitations and areas for future research applicable to this study before the chapter is concluded with some “final words”.

12.1 Reviewing the problem and objectives

This research was initiated by the idea of establishing an incident response capability for the South African NREN. When embarking on the journey to find out where to start, it was soon discovered that there does not appear to be a clear, consistent method or model for doing this. The problems addressed by this research are therefore:

1. The lack of a definitive method for establishing a CSIRT (in general).
2. The lack of an incident response capability in the SA NREN environment.

To address these problems, a number of research objectives were defined (section 1.5, page 10). These objectives are mapped to the chapters where they are achieved in this dissertation in table 12.1.

Table 12.1: Research objectives matched to dissertation chapters

Objective	Chapter(s)
Define CSIRTs and describe their services	3
Determine the requirements for establishing a CSIRT (state-of-the-art exploration)	4-7
Develop a generic model for establishing a CSIRT	8-9
Implement the model in the SA NREN environment	10-11

Briefly, CSIRTs and their services were defined and described in chapter 3. The CSIRT state-of-the-art was explored by identifying the requirements for establishing a CSIRT through the lens of ITIL's four Ps — People, Processes, Product and Partners — in chapters 4 to 7. A generic model for establishing a CSIRT was subsequently developed in chapters 8 and 9. Finally, the model was applied in the SA NREN environment as a demonstration of its utility (chapters 10 and 11).

12.2 Reflections on the research

This section considers the key findings of this study, the effectiveness of the methodology used as well as the resulting conclusions from each chapter. In addition, a brief assessment of how the model addresses the challenges when establishing a CSIRT is presented.

12.2.1 Key findings

The primary findings of this research are centred around the original objectives. CSIRTs were found be to the primary mechanism used to deal with IT security incidents today. The requirements for establishing a CSIRT were explored and successfully grouped according to the business requirements, services and four Ps proposed by ITIL. Based on these requirements, the relationships between the Ps were uncovered and eventually combined to form a generic model for establishing a CSIRT. This model addressed the business requirements, team model and staffing, policies and processes, tools and technologies, services, and partner aspects related to CSIRT establishment; thereby facilitating an holistic approach.

The model commenced with business requirements, followed with a natural progression through the people, policies and processes, and product requirements. Services and partners were developed incrementally in parallel with these last three categories. Finally, two views of the complete model were presented: a) a strategic view focusing on the business requirements, and b) a tactical view focusing on the four Ps plus services.

To demonstrate the utility of the model, it was instantiated in the SA NREN environment. This was preceded by a survey used to show the need for a CSIRT capability in this environment. The outcome of the survey was that CSIRT services would be more than useful to the community, but, interestingly enough, the most useful services were revealed to be the proactive rather than the reactive ones. Necessary information on the SA NREN environment, needed to make the decisions required for implementing the model, was solicited by relevant questions. The model was successfully "executed" to produce a specific model for a SA NREN CSIRT. Implementing this design should result in an incident response capability for the SA NREN satisfying the expectations of the community.

12.2.2 Methodology

Design Science Research (DSR) was selected as the primary methodology for this research. A survey accompanied this to enable the successful demonstration of the developed artefact.

Meeting the guidelines for DSR

Guidelines for performing DSR were presented in section 2.3.3 (page 27). This research meets these guidelines as shown in table 12.2.

Table 12.2: Satisfying the guidelines for DSR (by author)

	Guideline	Satisfied by
1	Design as an artefact	Producing a model for establishing a CSIRT
2	Problem relevance	Showing the need for a CSIRT within the SA NREN environment
3	Design evaluation	Demonstrating utility in the environment
4	Research contributions	Exercising the model in the SA NREN environment
5	Research rigour	Effective application of the knowledge base (constructs & framework)
6	Design as a search process	Using a concept matrix and in depth study of the literature
7	Communication of research	This dissertation and related reports published on the SANReN website

The first artefact produced by this research is a generic model for establishing a CSIRT (guideline one). According to Hevner et al. (2004, p. 79), relevance is assured by addressing a business need through research activities; in this case the need for a CSIRT for the SA NREN (guideline two). This need is confirmed by the survey results presented in chapter 10. A demonstration of the utility of the model is used as the evaluation method in chapter 11, showing that the model works (guideline three). Regarding guideline four, research contributions, it is argued that significant value to the research community is produced by exercising the artefact in the intended environment (Hevner et al., 2004, p. 87). This is achieved primarily in chapter 11.

Rigour (guideline five) can be shown through the extensive literature analysis that was performed illustrating “effective use of the knowledge base” (Hevner et al., 2004, p. 88). Rigour is further demonstrated through exercising the model in the SA NREN environment (Hevner et al., 2004, p. 88). In addition, it is argued that “rigor is achieved by appropriately applying existing foundations and methodologies” (Hevner et al., 2004, p. 80). Thus, the use of existing constructs from authoritative literature to define a framework for this research (chapter 2). The search process (guideline six), determining the requirements for CSIRTs from literature, is detailed in section 2.2 (page 17). Finally, this research, and the resulting artefacts, are communicated via this dissertation (and hopefully in subsequent publications) (guideline seven). Furthermore, preliminary findings have been communicated to both management and technical audiences through published reports on the SANReN website as shown in table 12.3.

DSR proved to be an effective methodology for executing this study. The process allowed for logical progression with a familiar “engineering” feel and the clear framework helped to scope the research. DSR further encouraged full circle research from *building* an artefact through to *evaluating* it.

Evaluating the model

Hevner et al. (2004, p. 86) summarise common design evaluation methods of artefacts. The methods most suited to the scope of this study are the descriptive methods, i.e. informed argument and scenarios. Existing information from related research forms the foundation of the model (chapters 3 to 7), thereby presenting a strong argument for the artefact’s utility. Additionally, a detailed scenario centred around the SA NREN environment is used to demonstrate the model’s utility (chapter 11).[1]

[1] As a SANReN engineer, I have detailed insight into the nature of the SA NREN environment. This knowledge was beneficial when it came to implementing the model. Throughout this dissertation, and especially in chapter 11, I have attempted to reveal and rationalise this knowledge as far as can be reasonably expected, providing reference to documents and reports where possible. The rest of the information should be regarded as obtained via personal communications with the respective personnel of the SANReN competency area and TENET staff.

Table 12.3: CSIRT reports published on the SANReN website (by author)

Title	Web address
Introduction to CSIRTs	`http://www.sanren.ac.za/wp-content/uploads/2012/11/SANReN_CSIRT_Introduction.pdf`
Security Incident Response for the South African NREN: Background, Survey & Problem Statement	`http://www.sanren.ac.za/wp-content/uploads/2012/11/IRT_background_survey_problem_SANReN.pdf`
SA NREN CSIRC Model: Computer Security Incident Response Capability	`http://www.sanren.ac.za/wp-content/uploads/2013/05/SA_NREN_CSIRC_Model-Published.pdf`

(Note: If these links are no longer functional please email rmooi@csir.co.za for a copy of the reports.)

Instantiating the model

The specific instantiation approach consisted of the following steps:

1. Identify a suitable environment — the SA NREN as per chapter 1.
2. Survey the environment (gather information required to implement the model) — presented in chapter 10.
3. Demonstrate the use of the model in the SA NREN — see chapter 11.

Executing these steps fulfils the *demonstrate* and *evaluate* activities of the design science research process from the previous section.

12.2.3 Addressing the challenges when establishing a CSIRT

As part of the initial literature survey, several challenges were identified that may be encountered when establishing a CSIRT (see section 3.1.1, page 32). Although the objective of this research was not to necessarily address these challenges, it is well worth the time to reflect on the extent by which these challenges are addressed by the model. Therefore, these challenges are repeated in this section with the aim of informally assessing how the model addresses them. The challenges and the corresponding means by which they are addressed, using the generic model for establishing a CSIRT, are shown in table 12.4.

The model addresses most of these challenges directly by stipulating the requirement for explicit information (e.g. mission, roles and responsibilities, funding, etc.). Some of the more obscure challenges and how they are addressed are discussed in the following paragraphs.

The challenge of a *lack of management support* needs to be addressed prior to commencing the design of the CSIRT; as such, it is outside of the domain of the model. The model therefore assumes that management support is in place for the CSIRT to be successfully implemented. *Bad publicity* is addressed through clear descriptions of the relationships between the media and the areas for establishment. Policies and processes for interacting with the press are advised and these will stipulate the circumstances and nature of media interactions. For example, working through a media point-of-contact, who is properly briefed and trained in media interactions, will mitigate the risk of bad publicity. Clear and timely communications with the constituency and partners is also crucial.

Table 12.4: Addressing the challenges when establishing a CSIRT

Challenge	Addressed by	Section
Unclear mandate	Environment: mission	9.1.1
Ill-defined roles and responsibilities	Staff and Policies: roles and responsibilities	9.3.1
Lack of management support	*Required prior to starting the design	N/A
Bad publicity	Staff, Policies & Processes, Partners: media	9.3
Finding investments	Funding/Budget	9.1.3
Amount of equipment required	Tools & Technologies supported by Funding	9.3.3, 9.1.3
Restrictive host organisation policies	Relationship with internal Partners + compliant Policies	9.3.2
Determining the service hours	Team model: work schedule	9.3.1
Insufficient staff (numbers)	Team model: staff numbers	9.3.1
Selecting a revenue model	Funding/Budget	9.1.3
Choosing the CSIRT services	Services	9.2
Understanding the processes	Policies & Processes	9.3.2
Untested procedures which may fail	Processes based on existing models	9.3.2
Interacting with constituency + external parties	Tools & Technologies supporting interactions	9.1.2, 9.3.4

The challenge of *restrictive host organisation policies* is addressed by having a good relationship with internal partners (especially the IT department), as well as CSIRT policies that are based on and compliant with those of the host organisation (following the recommendations by Grobler and Bryk (2010)). Finally, the risk of *untested procedures which may fail*, is alleviated by using CSIRT processes based on best practice methods from literature, reflecting processes that work in real life.

12.2.4 Summary of conclusions

From this work as a whole, it can be deduced that it is possible to develop a generic model for establishing a CSIRT. Furthermore, this model was successfully instantiated in the context of the SA NREN showing its effectiveness in at least one environment. These artefacts link back to and address the problems of a deficiency in both a standard model for CSIRT establishment as well as the need for incident response within the SA NREN.

In the first chapter, IT security incidents and CSIRTs, as a mechanism for dealing with these incidents, were introduced. In addition, background was provided on the SA NREN environment, setting the scene for the problem area, problem statement and research objectives. The chapter was concluded with the layout for the dissertation.

Chapter 2 described the methodology used for conducting this research. The literature survey, approach used for developing the model, and the implementation thereof, were each described in turn. Design science research, as the primary method, appears to have suited the research well.

The next part of the dissertation presented the results of the literature survey through a framework based on the four Ps from the IT Infrastructure Library (ITIL). Chapter 3, CSIRTs today, acted as a background to CSIRTs by introducing typical CSIRT services before moving on to the basic business requirements for establishing a CSIRT. These were identified in five groups: the environment, constituency, funding, legal considerations and authority. Specific decisions (or questions that need to be answered) for each group of business requirements were expressed. The approach used to discuss the subsequent requirements according to ITIL's four Ps was then introduced before concluding the chapter.

Chapters 4 to 7 described the requirements for CSIRTs under each of these categories: People, Processes, Products and Partners, respectively. The first of these chapters found that the team model needs to be determined prior to other staffing considerations. Thereafter, the following needed to be considered: staff numbers, work schedules, roles, responsibilities and required skills. Chapter 5 covered CSIRT policies and processes, discussing the core ones in detail and summarising the others that may be needed depending on the circumstances. The next chapter focused on the services provided by CSIRTs as well as the tools and technologies required for operations. Each possible CSIRT service was described, followed by tools and technologies used to support these services. Rounding off this part is chapter 7, briefly uncovering the various internal and external partners involved in CSIRT activities.

Part III contains two chapters wherein the generic model for establishing a CSIRT is developed. The first, chapter 8, explores the relationships between the Ps from the previous chapters as revealed by the literature study. These relationships are summarised in figure 8.16 (page 122). Chapter 9 brings the previous chapters together to build the generic model for establishing a CSIRT. This is achieved through the use of a framework based on ITIL's business-driven technology management areas supplemented with partners and services on each side (see figure 9.2, page 127). Each area is explored consecutively, highlighting the relevant questions that need to be answered prior to moving on to the next area. The links to other areas and resultant effects are subsequently discussed. These are all combined to form a complete model for establishing a CSIRT from both a strategic and tactical perspective (as shown in figures 9.19 and 9.20, pages 144 and 145).

The next part aims to demonstrate the use of this model in the SA NREN environment. To do that, the current state of affairs regarding incident response mechanisms needed to be determined. This was achieved via the use of a survey (chapter 10). Analysis of the results showed that there was indeed a need for a CSIRT. Additionally, focus should be given to proactive and security quality management services targeted at reducing the likelihood of incidents on the SANReN network, as the "most useful services". Another interesting outcome was the variance in the most useful services for science/research institutions and universities respectively. Whereas the universities preferred training and security consulting services, the science/research institutions preferred security audits and information dissemination.

The argument for coordination was further strengthened by the presence of existing security teams in the constituency. This information was useful for making the decisions required to instantiate the generic model in the SA NREN environment.

Chapter 11 executed this model to design the specific model for a CSIRT in the SA NREN. Each question from chapter 9 was addressed and answered as far as possible for the SA NREN environment. The carry-on effect to the other areas was explained as the execution progressed through each phase until the model was successfully completed. This showed that the model *could* work and resulted in an holistic design for the SA NREN CSIRT.

12.3 Research contributions

Ultimately, this research satisfies its aim by providing a model for the SA NREN CSIRT. To do this, a generic model for establishing a CSIRT first needed to be developed. These two artefacts are the primary deliverables and research contributions of this study; shown in context of the DSR framework in figure 12.1 (complementing figure 2.2 page 24). The primary contributions and possible uses thereof are described in this section.

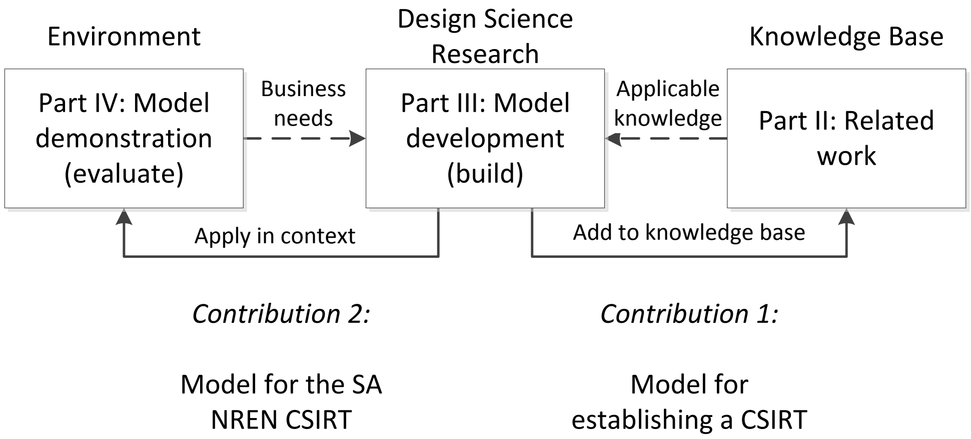


Figure 12.1: DSR framework showing research contributions (by author)

Firstly, prior to this research, no consistent model for establishing a CSIRT was apparent. There are existing methods such as those proposed by ENISA (2006) and Killcrece (2004) but these seemed lacking in either completeness or detail. Furthermore, no clear alignment with other CSIRT literature makes it difficult to evaluate and compare these methods. If there are two or more different methods for achieving the same thing, where does one start?

This research attempts to resolve this confusing situation by providing a clear and complete model for new teams to establish a CSIRT, based on primary CSIRT literature. It may also be useful for comparing existing incident response capabilities in terms of the relationships between the Ps and identifying possible areas for improvement. In addition, by bringing together the prior literature to assess the state-of-the-art and CSIRT best practices, this research is valuable as a literature survey, providing a good list of resources for CSIRT establishment teams to consult. Furthermore, the similarities and differences between each resource are highlighted throughout the dissertation, showing both requirements agreed on by multiple authors as well as those mentioned by just one or two authors. Combining these resources and identifying the commonalities meant that consistency of the model could be achieved.

12.4 Limitations and future research

This section presents the limitations of this research and subsequent ideas for enhancing the model. It focuses on generalisability of the model, further evaluation through case studies, expert interviews and comparison with proposed methods for establishing a CSIRT. These four limitations are described in the remainder of this section.

12.4.1 Generalisability

The model was successfully demonstrated in the SA NREN environment, hinting that it could work in other NREN or even dissimilar environments. Limitations of the instantiation approach however, as a single demonstration, include generalisability of the model.

One of the challenges of DSR is that "artifact performance is related to the environment in which it operates" (March & Smith, 1995, p. 254). This can result in an unsuitable artefact or one with unwanted side-effects. Further research, i.e. implementing the CSIRT model in different environments, can show the suitability of this model for those environments. These studies can possibly be performed through the use of the case study method (Hevner et al., 2004, p. 86).

12.4.2 Evaluation

This model can be expanded into a method for establishing a CSIRT as "a set of steps used to perform a task" (March & Smith, 1995, p. 257). Either this model or subsequent methods can be compared to the processes recommended by CSIRT literature such as ENISA (2006) and Killcrece (2004). (Note though that the recommendations from the step-by-step guide (ENISA, 2006) were already integrated into this research as one of the primary sources for the model.) This can be seen as comparing the solution "with those constructed by expert human designers for the same problem situation" (Hevner et al., 2004, p. 90) with the purpose of measuring the effectiveness of the model.

12.4.3 Comparability

In addition, to strengthen the evaluation, the previous comparison can be used to position the model with respect to existing models/methods (March & Smith, 1995, p. 261). Although, in the absence of known metrics for comparing these models, this could be challenging. For example, how can "significant improvement" (March & Smith, 1995, p. 260) be evaluated? In other words, suitable metrics would likely need to be developed prior to conducting such research.

12.4.4 Completeness

Further research possibilities emerge from these limitations. As explained, these include case studies of implementing the model with appropriate metrics to evaluate its effectiveness. Feedback from these case studies, to suggest improvements, can be applied to the model by cycling through the DSR build and evaluate processes until the model is suitably refined.

This can be complemented by interviews or focus groups with CSIRT experts asked to examine and evaluate the model. This has the advantage of providing quicker feedback than case studies with opportunity to refine the model (re-iterate it from the feedback received) prior to implementation.

12.4.5 Other ideas

Other areas of future research could include more detailed exploration of requirements pertaining to the individual Ps; for example, specific policies and procedures, and how they interact with other Ps.

Finally, a complementary model for establishing a CSIRT could be developed based on the COBIT[2] 5 Enablers (ISACA, 2012, p. 27). This could be used to highlight gaps in the generic model by providing an alternative model centred around principles, policies and frameworks (the first enabler). The addition of information as well as culture, ethics and behaviour, as aspects not considered in this dissertation, could prove insightful. These enablers are highlighted in figure 12.2.

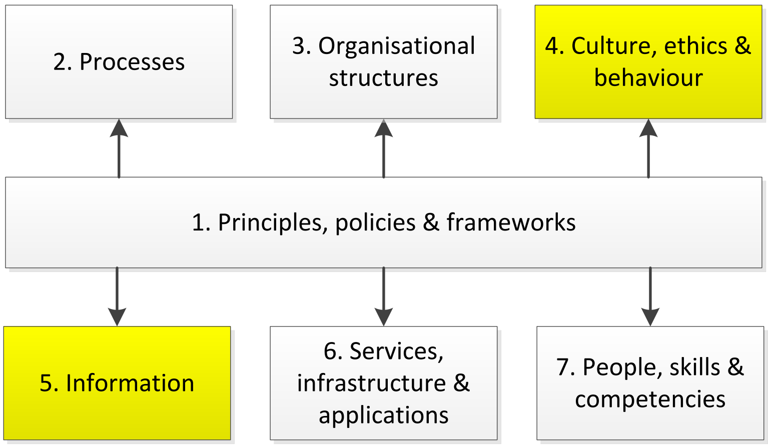

2. Processes
3. Organisational structures
4. Culture, ethics & behaviour
1. Principles, policies & frameworks
5. Information
6. Services, infrastructure & applications
7. People, skills & competencies

Figure 12.2: COBIT 5 Enablers (adapted from ISACA (2012, p. 27))

Finally, limitations of the survey instrument are discussed in section 10.4 (page 158). As an alternative or complement to the survey, interviews with a selected sample of the population could reveal the reason for certain survey outcomes (e.g. the importance/usefulness of specific services).

[2] The Control Objectives for Information and Related Technologies (COBIT®) is a globally accepted "framework for the governance and management of enterprise IT" (see `http://www.isaca.org/COBIT/Pages/COBIT-5-Framework-product-page.aspx`).

12.5 Final words

Hevner et al. (2004, p. 85) argue that “a design artifact is complete and effective when it satisfies the requirements and constraints of the problem it was meant to solve”. The problem addressed by this dissertation is the lack of an incident response capability for the SA NREN; the solution, two artefacts:

1. a generic model for establishing a CSIRT, and
2. a specific model for the SA NREN CSIRT.

The generic model was found to be both useful and satisfactory. Implementing the specific design will result in the establishment of the SA NREN CSIRT based on the knowledge that all of the areas revealed through this research have been addressed. This provides reassurance that nothing has been left out.

As the saying goes, “the proof is in the pudding”. The real test for this research will be the implementation of the design and subsequent assessment of the *new* state-of-affairs to establish whether anything is missing from the design. Another iteration of the build-evaluate process may follow or otherwise the design can be stamped “complete”. Time will tell...

Part VI

Appendices

Appendix A

Terms and definitions

IT security incident

"a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security" (SANS, 2009, p. 3).

Computer Security Incident Response Team (CSIRT)

"an organization or team that provides services and support to a defined constituency for preventing, handling, and responding to computer security incidents" (Alberts et al., 2004, p. 1).

Constituency

"the group of users, sites, networks or organisations served by the team" (Brownlee & Guttman, 1998, p. 17). I.e. *"the customer base of a CSIRT"* (ENISA, 2006, p. 7).

National Research and Education Network (NREN)

"a specialised Internet service provider to the research and educational communities within a country" (TERENA, 2010, para. 8).

Policies

"the governing principles under which the team operates" (West-Brown et al., 2003, p. 21).

Process

"a structured set of activities designed to accomplish a specific objective" (Hunnebeck, 2011, p. 412).

Technology

"The application of scientific knowledge for practical purposes" (`http://www.oxforddictionaries.com/definition/english/technology`).

Tool

"A device or implement... used to carry out a particular function" (`http://www.oxforddictionaries.com/definition/english/tool`).

Appendix B

Detailed literature concept matrix

Table B.1: Literature concept matrix (part 1: Business requirements)

	Constituency	Mission	Legal	Authority	Funding
Alberts et al. (2004)		✓	✓		
Brownlee and Guttman (1998)	✓		✓	✓	
Cichonski et al. (2012)	✓				
ENISA (2006)	✓	✓			✓
Killcrece et al. (2003a)	✓	✓		✓	
Killcrece et al. (2003b)		✓	✓	✓	✓
ENISA (2010)	✓✓	✓	✓		
Northcutt (2003)					
Penedo (2006)		✓			
Smith (1994)	✓	✓	✓	✓	✓
West-Brown et al. (2003)	✓	✓	✓	✓	✓

Table B.2: Literature concept matrix (part 2: People)

	Team Model	Staffing	Roles	Skills
Alberts et al. (2004)			✓✓	
Brownlee and Guttman (1998)				
Cichonski et al. (2012)	✓	✓	✓	✓
ENISA (2006)	✓✓	✓	✓	✓
Killcrece et al. (2003a)	✓✓		✓	
Killcrece et al. (2003b)	✓	✓	✓✓	
ENISA (2010)	✓\	✓	✓	✓
Northcutt (2003)			✓	✓\
Penedo (2006)				
Smith (1994)		✓	✓\	✓
West-Brown et al. (2003)		✓		✓

Table B.3: Literature concept matrix (part 3: Policies & processes)

	Policy	Processes	Incident Handling
Alberts et al. (2004)		✓✓	
Brownlee and Guttman (1998)	✓\		
Cichonski et al. (2012)	✓	✓	
ENISA (2006)	✓	✓\	✓✓(+alerts)
Killcrece et al. (2003a)	✓	✓\	
Killcrece et al. (2003b)	✓\	✓✓	✓
ENISA (2010)	✓✓	✓\	✓✓
Northcutt (2003)		✓	✓
Penedo (2006)			
Smith (1994)	✓✓	✓	
West-Brown et al. (2003)	✓✓	✓✓	

Table B.4: Literature concept matrix (part 4: Other)

	Services	Tools and Technologies	Partners
Alberts et al. (2004)	✓^	✓	✓
Brownlee and Guttman (1998)	✓	✓	✓
Cichonski et al. (2012)	✓^	✓	✓
ENISA (2006)		✓	✓^
Killcrece et al. (2003a)	✓✓	✓	✓
Killcrece et al. (2003b)	✓	✓✓	✓
ENISA (2010)	✓	✓✓	✓
Northcutt (2003)		✓	✓
Penedo (2006)		✓✓	
Smith (1994)	✓^	✓	✓
West-Brown et al. (2003)	✓✓	✓✓	✓

Appendix C

Traffic light protocol for information sharing

The traffic light protocol (TLP) is used by CSIRTs to indicate how sensitive or not information is and accordingly, how it should be handled and shared[1]. The four categories of the TLP as well as a proposed mapping to the scheme proposed by (Smith, 1994) are shown in table C.1. Note that "classified" data is usually handled outside of the TLP[1].

[1] http://www.us-cert.gov/tlp

Table C.1: Traffic light protocol (adapted from[a,b,c,d])

Colour	When information…	Can be shared…	Maps to
White	can be freely circulated, released publicly and is subject to zero or minimal risk of misuse.	without restriction subject to original copyright.	Public
Green	is not intended for broad Internet (public) circulation, (is not particularly sensitive) and is useful for constituency and partner awareness.	freely with the entire community (constituency and partners) but not published on the web.	Sensitive
Amber	should be limited in disclosure to a specific group and could carry risks to privacy, reputation or operations if shared externally.	with members of the same community, organisation or exchange as applicable and appropriate. Restrictions can be specified by originator.	Private
Red	is personal or confidential (for privacy or security reasons), intended for the direct recipients only and should not be disclosed to anyone else.	never. It is restricted to the initial participants of the exchange, meeting or conversation and should not be disseminated outside this group.	Highly sensitive

[a] `http://www.us-cert.gov/tlp`

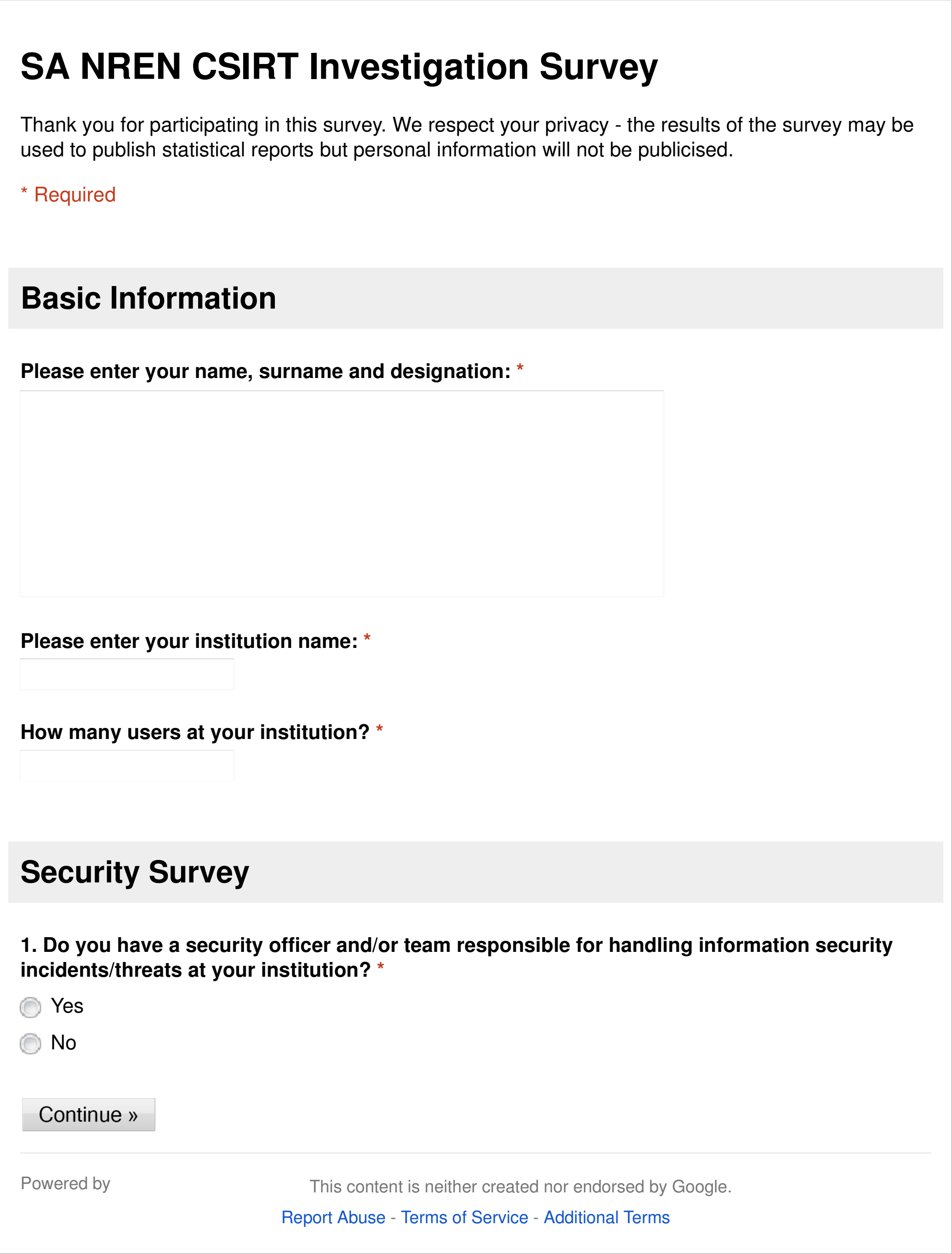
[b] `http://www.surf.nl/en/services-and-products/surfcert/information-sharing-traffic-light-protocol/index.html`

[c] `http://www.terena.org/activities/tf-csirt/publications/ISTLP-v1.1.pdf`

[d] `https://www.cert.be/traffic-light-protocol-tlp`

Appendix D

SA NREN CSIRT survey



SA NREN CSIRT Investigation Survey

Thank you for participating in this survey. We respect your privacy - the results of the survey may be used to publish statistical reports but personal information will not be publicised.

* Required

Basic Information

Please enter your name, surname and designation: *

Please enter your institution name: *

How many users at your institution? *

Security Survey

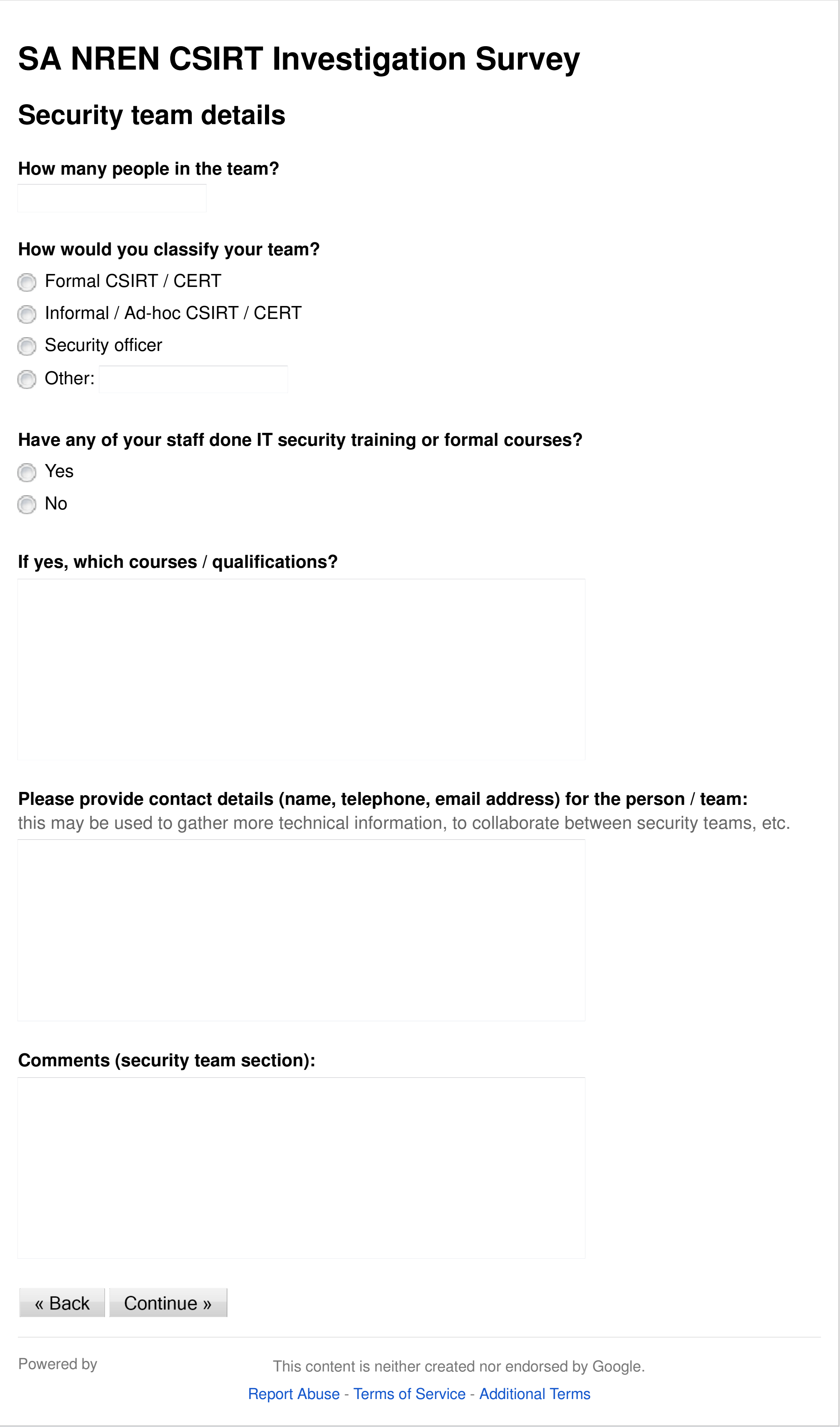
1. Do you have a security officer and/or team responsible for handling information security incidents/threats at your institution? *

○ Yes

○ No

Continue »
Powered by
This content is neither created nor endorsed by Google.
Report Abuse - Terms of Service - Additional Terms

Figure D.1: Survey page 1: Basic information + Security survey



SA NREN CSIRT Investigation Survey

Security team details

How many people in the team?

How would you classify your team?

○ Formal CSIRT / CERT

○ Informal / Ad-hoc CSIRT / CERT

○ Security officer

○ Other:

Have any of your staff done IT security training or formal courses?

○ Yes

○ No

If yes, which courses / qualifications?

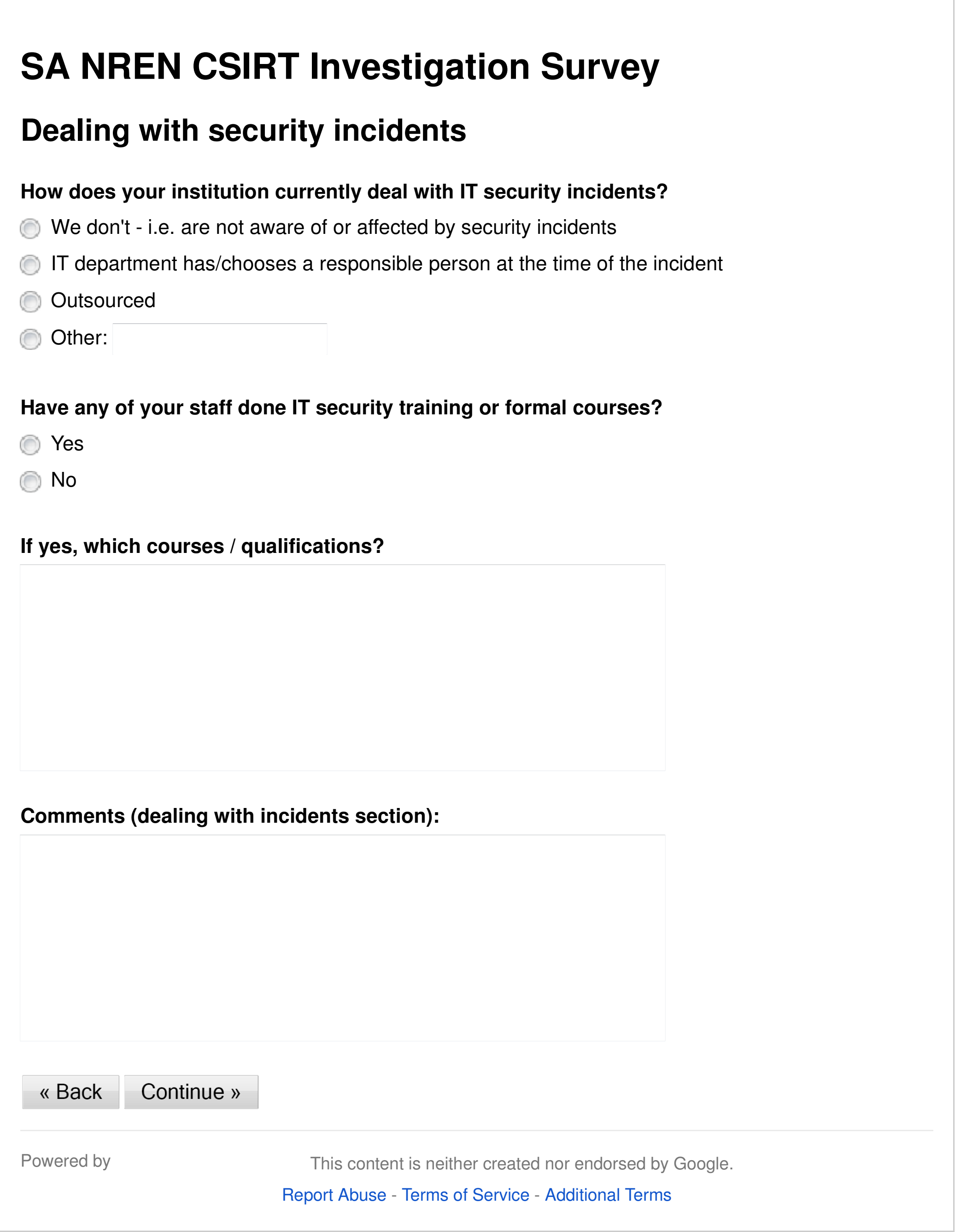
Please provide contact details (name, telephone, email address) for the person / team:

this may be used to gather more technical information, to collaborate between security teams, etc.

Comments (security team section):

« Back
Continue »
Powered by
This content is neither created nor endorsed by Google.
Report Abuse - Terms of Service - Additional Terms

Figure D.2: Survey page 2 (option 1): Security team details



SA NREN CSIRT Investigation Survey

Dealing with security incidents

How does your institution currently deal with IT security incidents?

○ We don't - i.e. are not aware of or affected by security incidents

○ IT department has/chooses a responsible person at the time of the incident

○ Outsourced

○ Other:

Have any of your staff done IT security training or formal courses?

○ Yes

○ No

If yes, which courses / qualifications?

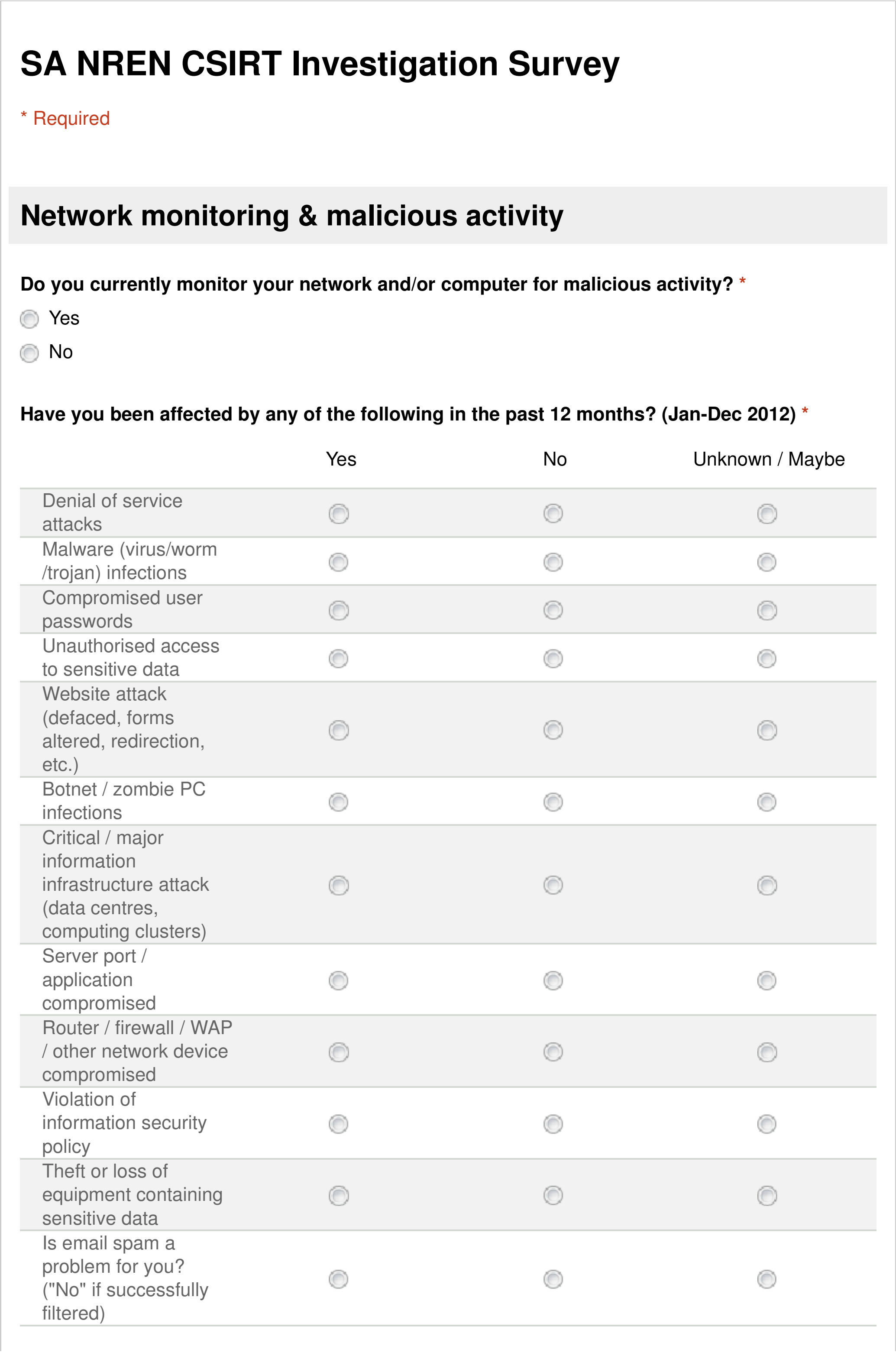
Comments (dealing with incidents section):

Powered by

This content is neither created nor endorsed by Google.

Report Abuse - Terms of Service - Additional Terms

Figure D.3: Survey page 2 (option 2): Dealing with security incidents



SA NREN CSIRT Investigation Survey

* Required

Network monitoring & malicious activity

Do you currently monitor your network and/or computer for malicious activity? *

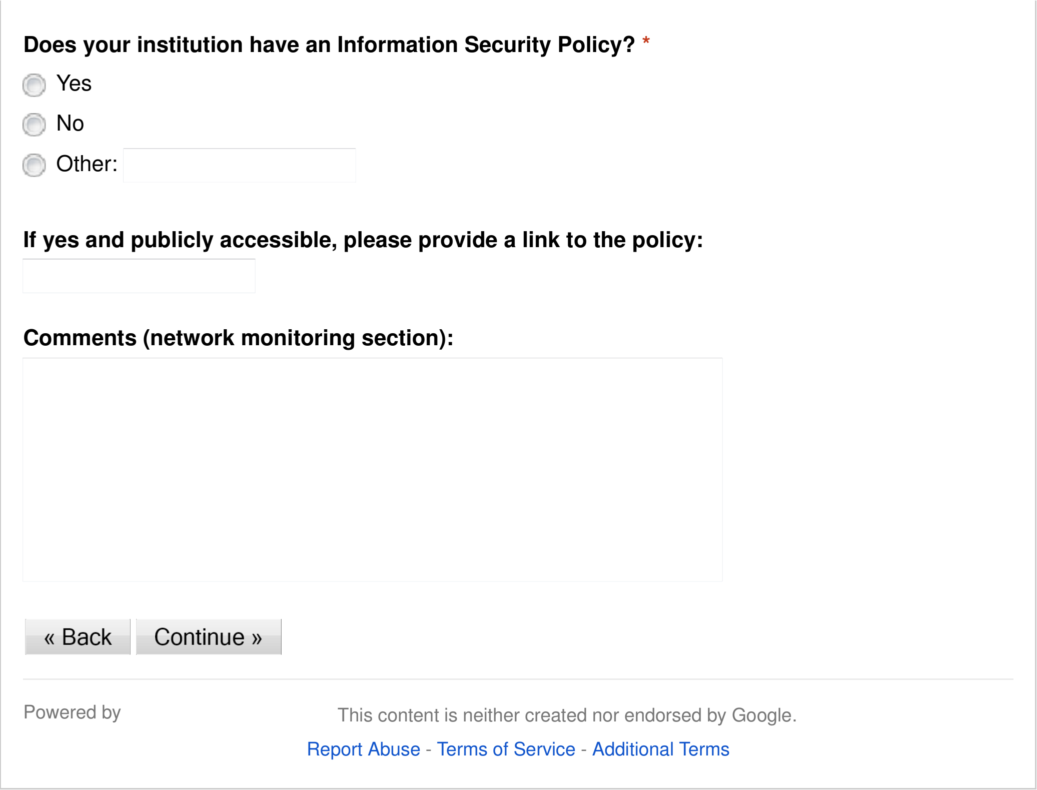
○ Yes

○ No

Have you been affected by any of the following in the past 12 months? (Jan-Dec 2012) *

	Yes	No	Unknown / Maybe
Denial of service attacks	○	○	○
Malware (virus/worm /trojan) infections	○	○	○
Compromised user passwords	○	○	○
Unauthorised access to sensitive data	○	○	○
Website attack (defaced, forms altered, redirection, etc.)	○	○	○
Botnet / zombie PC infections	○	○	○
Critical / major information infrastructure attack (data centres, computing clusters)	○	○	○
Server port / application compromised	○	○	○
Router / firewall / WAP / other network device compromised	○	○	○
Violation of information security policy	○	○	○
Theft or loss of equipment containing sensitive data	○	○	○
Is email spam a problem for you? ("No" if successfully filtered)	○	○	○

Figure D.4: Survey page 3a: Network monitoring & malicious activity



Does your institution have an Information Security Policy? *

○ Yes

○ No

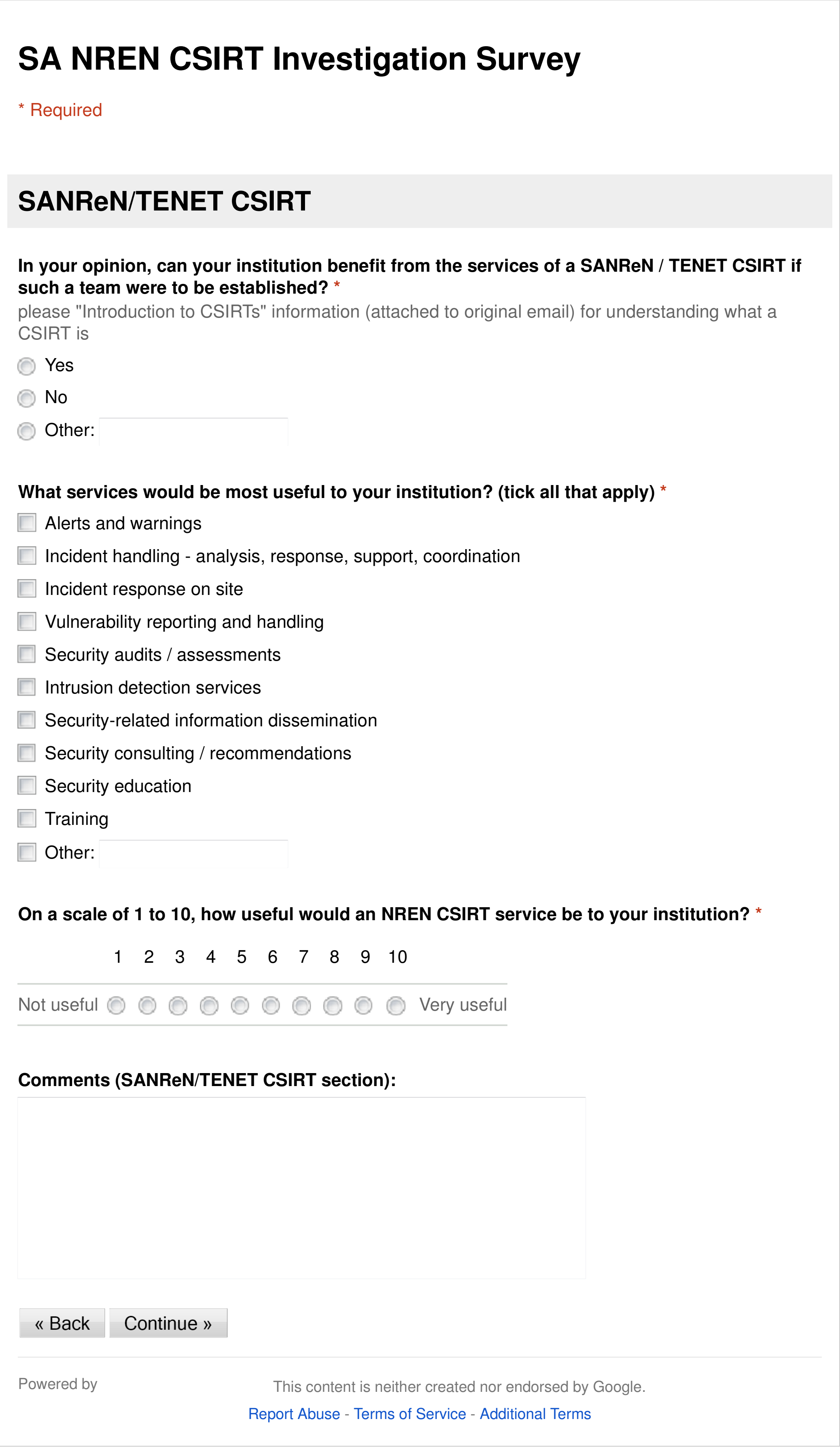
○ Other:

If yes and publicly accessible, please provide a link to the policy:

Comments (network monitoring section):

« Back
Continue »
Powered by
This content is neither created nor endorsed by Google.
Report Abuse - Terms of Service - Additional Terms

Figure D.5: Survey page 3b: Network monitoring & malicious activity (continued)



SA NREN CSIRT Investigation Survey

* Required

SANReN/TENET CSIRT

In your opinion, can your institution benefit from the services of a SANReN / TENET CSIRT if such a team were to be established? *

please "Introduction to CSIRTs" information (attached to original email) for understanding what a CSIRT is

○ Yes

○ No

○ Other:

What services would be most useful to your institution? (tick all that apply) *

□ Alerts and warnings

□ Incident handling - analysis, response, support, coordination

□ Incident response on site

□ Vulnerability reporting and handling

□ Security audits / assessments

□ Intrusion detection services

□ Security-related information dissemination

□ Security consulting / recommendations

□ Security education

□ Training

□ Other:

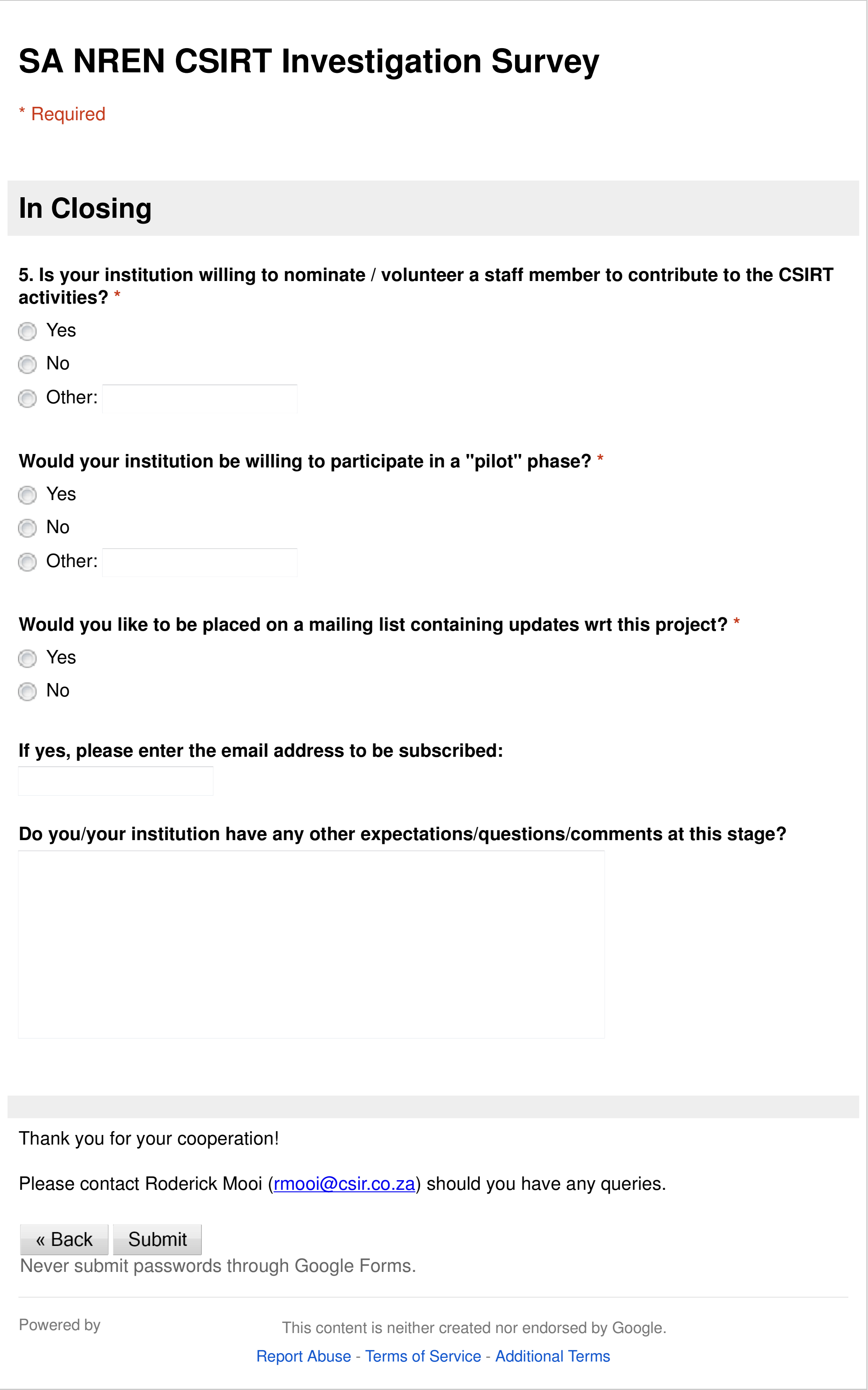
On a scale of 1 to 10, how useful would an NREN CSIRT service be to your institution? *

	1	2	3	4	5	6	7	8	9	10	
Not useful	○	○	○	○	○	○	○	○	○	○	Very useful

Comments (SANReN/TENET CSIRT section):

« Back
Continue »
Powered by
This content is neither created nor endorsed by Google.
Report Abuse - Terms of Service - Additional Terms

Figure D.6: Survey page 4: SANReN/TENET CSIRT



SA NREN CSIRT Investigation Survey

* Required

In Closing

5. Is your institution willing to nominate / volunteer a staff member to contribute to the CSIRT activities? *

○ Yes

○ No

○ Other:

Would your institution be willing to participate in a "pilot" phase? *

○ Yes

○ No

○ Other:

Would you like to be placed on a mailing list containing updates wrt this project? *

○ Yes

○ No

If yes, please enter the email address to be subscribed:

Do you/your institution have any other expectations/questions/comments at this stage?

Thank you for your cooperation!

Please contact Roderick Mooi (rmooi@csir.co.za) should you have any queries.

Never submit passwords through Google Forms.

Powered by

This content is neither created nor endorsed by Google.

Report Abuse - Terms of Service - Additional Terms

Figure D.7: Survey page 5: In closing

Bibliography

Alberts, C., Dorofee, A., Killcrece, G., Ruefle, R., & Zajicek, M. (2004). *Defining incident management processes for CSIRTs : A work in progress* (Tech. Rep.). Carnegie Mellon University. (Retrieved 13 February, 2013 from `www.sei.cmu.edu/reports/04tr015.pdf`)

Brownlee, N., & Guttman, E. (1998, June). *Expectations for computer security incident response.* RFC 2350 (Best Current Practice). IETF. (Retrieved May 10, 2012 from `http://www.ietf.org/rfc/rfc2350.txt`)

Callas, J., Donnerhacke, L., Finney, H., Shaw, D., & Thayer, R. (2007, November). *OpenPGP message format.* RFC 4880 (Standards Track). IETF. (Retrieved Feb 18, 2015 from `https://tools.ietf.org/html/rfc4880`)

Cannon, D. (2011). *ITIL® service strategy.* London: The Stationary Office (TSO).

Carnegie Mellon University. (2006). *Action list for developing a computer security incident response team (CSIRT).* (Retrieved February 27, 2012 from `http://www.cert.org/csirts/action_list.html`)

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). *Computer security incident handling guide* (Special Publication 800-61. Revision 2). NIST. (Retrieved 12 September, 2012 from `http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf`)

DHET. (2013). *Statistics on post-school education and training in South Africa: 2011* (Tech. Rep.). Department of Higher Education and Training. (Retrieved October 30, 2014 from `http://www.dhet.gov.za/DHETStatisticsPublication/Statisticsonpost-schooleducationandtraininginSouthAfrica2011.pdf`)

DoC. (2010, February). *Electronic Communications Act (36/2005): Notice of intention to make South African national cybersecurity policy.* Government gazette. (No. 32963. Department of Communications. Retrieved February 29, 2012 from http://www.pmg.org.za/node/20036)

Ellefsen, I., & von Solms, S. (2010). The community-orientated computer security, advisory and warning team. In *IST-Africa 2010 conference proceedings.*

ENISA. (2006). *A step-by-step approach on how to set up a CSIRT* (Tech. Rep.). ENISA. (Retrieved January 25, 2012 from http://www.enisa.europa.eu/activities/cert/support/guide)

ENISA. (2010). *Good practice guide for incident management* (Tech. Rep.). ENISA. (Retrieved April 18, 2012 from http://www.enisa.europa.eu/act/cert/support/guide2)

ENISA. (2011, November). *Inventory of CERT activities in Europe* (No. 2.6). (Retrieved May 8, 2012 from http://www.enisa.europa.eu/activities/cert/background/inv/files/inventory-of-cert-activities-in-europe)

ENISA. (2014). *Biggest EU cyber security exercise to date: Cyber Europe 2014 taking place today.* (Retrieved from http://www.enisa.europa.eu/media/press-releases/biggest-eu-cyber-security-exercise-to-date-cyber-europe-2014-taking-place-today)

FIRST. (2012). *FIRST conference - about the conference.* (Retrieved March 2, 2012 from http://conference.first.org/about/index.aspx)

GÉANT. (2011). *GÉANT security - CERT portal.* (Retrieved April 19, 2012 from http://www.geant.net/Services/NetworkPerformanceServices/Pages/GEANTSecurity.aspx)

Grobler, M., & Bryk, H. (2010). Common challenges faced during the establishment of a CSIRT. In *2010 Information Security for South Africa conference.*

Grobler, M., Vuuren, J. van, & Leenen, L. (2012). Implementation of a cyber security policy in South Africa: Reflection on progress and the way forward. In M. Hercheui, D. Whitehouse, J. McIver, William, & J. Phahlamohlaka (Eds.), *ICT critical infrastructures and society* (Vol. 386, p. 215-225). Springer Berlin Heidelberg.

Guttman, B., & Roback, E. A. (1995). *An introduction to computer security: The NIST handbook.*

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Quarterly*, *28*(1), 75-105.

Hofstee, E. (2006). *Constructing a good dissertation.* EPE. (ISBN: 0958500711)

Hunnebeck, L. (2011). *ITIL® service design.* London: The Stationary Office (TSO).

ISACA. (2012). *COBIT® 5 framework.* ISACA. (Retrieved 13 April, 2012 from `http://www.isaca.org/COBIT/Pages/COBIT-5-Framework-product-page.aspx`)

ISSA. (2012). *Information Security South Africa 2012 conference.* (Retrieved February 28, 2012 from `http://www.infosecsa.co.za`)

Kácha, P. (2009). Adapting the ticket request system to the needs of CSIRT teams. *WSEAS Transactions on Computers*, *8*(9).

Killcrece, G. (2004). Steps for creating national CSIRTs. (August), 1–26.

Killcrece, G., Kossakowski, K.-P., Ruefle, R., & Zajicek, M. (2003a). *Organizational models for computer security incident response teams (CSIRTs)* (Tech. Rep.). Carnegie Mellon Software Engineering Institute.

Killcrece, G., Kossakowski, K.-P., Ruefle, R., & Zajicek, M. (2003b). *State of the practice of computer security incident response teams (CSIRTs)* (Tech. Rep.). Carnegie Mellon Software Engineering Institute.

Kumparak, G. (2014). *Massive security bug in OpenSSL could affect a huge chunk of the Internet.* (Retrieved from `http://www.techcrunch.com/2014/04/07/massive-security-bug-in-openssl-could-effect-a-huge-chunk-of-the-internet`)

March, S. T., & Smith, G. F. (1995). Design and natural science research on information technology. *Decision Support Systems*, *15*(4), 251-266.

Martin, D. (2012). *About TENET.* (Retrieved September 7, 2012 from `http://www.tenet.ac.za/about-us/About_TENET.pdf`)

News24. (2012, July). *US, Iran cyber war beginning.* (Retrieved August 27, 2012 from `http://www.news24.com/SciTech/News/US-Iran-cyber-war-beginning-20120713`)

Northcutt, S. (2003). *Computer security incident handling* (Version 2. ed.). SANS Press.

Olivier, M. S. (2008). *Information technology research* (3 ed.). Van Schaik. (ISBN: 9780627027581)

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of Management Information Systems*, *24*(4), 45-77.

Penedo, D. (2006). Technical infrastructure of a CSIRT. In *Proceedings of the international conference on internet surveillance and protection* (pp. 27–32). Washington, DC, USA: IEEE Computer Society.

Petruccione, F., Hazelhurst, S., Høst, G., Lourens, A., McIntyre, C., & Moore, R. (2013). *National Integrated Cyberinfrastructure System: A framework for the establishment and maintenance of a sustainable NICIS* (Tech. Rep.). Department of Science and Technology. (Retrieved June 18, 2014 from `http://www.dst.gov.za/images/NICIS_Framework_Report_December_2013_26_May_2014.pdf`)

Proctor, T. (2012). The development of cyber security warning, advice and report points. In *Secure IT systems* (pp. 61–72). Springer Berlin Heidelberg.

Ranger, S. (2014). *Inside the secret digital arms race: Facing the threat of global cyberwar.* (Retrieved from `http://www.techrepublic.com/article/inside-the-secret-digital-arms-race`)

Reuters. (2012, August). *Latest Java software leaves PCs vulnerable.* (Retrieved September 5, 2012 from `http://www.itweb.co.za/index.php?option=com_content&view=article&id=58034:latest-java-software-leaves-pcs-vulnerable&catid=234`)

SANReN. (2010). *Overview.* (Retrieved April 20, 2012 from `http://www.sanren.ac.za/overview`)

SANS. (2008). *Information technology - Security techniques - Code of practice for information security management* (1 ed.; Standard No. 27002). Standards South Africa.

SANS. (2009). *Information technology — Security techniques — Information security management systems — Overview and vocabulary* (Standard No. 27000). Standards South Africa.

Smith, D. (1994). Forming an Incident Response Team. In *FIRST annual conference proceedings* (pp. 1–37).

Staphorst, L. (2014, June). *SANReN annual report for 2013/14.* (Available from Makan, A., amakan@csir.co.za)

TENET. (2012a). *Acceptable use policy.* (Version 3.2. Retrieved September 23, 2014 from `http://www.tenet.ac.za/doc/aup-3-2.pdf/at_download/file`)

TENET. (2012b). *Connection policy.* (Version 3.1. Retrieved September 22, 2014 from `http://www.tenet.ac.za/doc/connection-policy/`)

TENET. (2013). *About TENET.* (Retrieved September 22, 2014 from `http://www.tenet.ac.za/about/about-tenet-1`)

TERENA. (2010, April). *Research and education networking FAQ.* (Retrieved May 4, 2012 from `http://www.terena.org/activities/development-support/r+e-faq/general.html`)

van Pinxteren, B. (Ed.). (2011). *TERENA compendium of national research and education networks in Europe* (2011 ed.). TERENA. (Retrieved May 8, 2012 from `http://www.terena.org/activities/compendium/2011/pdf/TER-C11-complete-web.pdf`)

Webster, J., & Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a literature review. *MIS Q.*, *26*(2), xiii–xxiii.

West-Brown, M. J., Stikvoort, D., Kossakowski, K.-P., Killcrece, G., Ruefle, R., & Zajicek, M. (2003). *Handbook for computer security incident response teams (CSIRTs)* (2 ed.). Carnegie Mellon SEI. (Retrieved 22 February, 2012 from `http://www.cert.org/archive/pdf/csirt-handbook.pdf`)