The University of the Western Cape

Faculty of Commerce

Proposing a Maturity Assessment Model Based on the digital forensic readiness Commonalities Framework

A mini-thesis submitted in partial fulfilment of the requirements for the degree of Magister Commercii in Information Management in the Department of Information Systems of the University of the Western Cape.

Presented by

Ivan Prins Claims

Student No: 3013430

Supervisor Dr F Bankole

ABSTRACT

The purpose of the study described in this thesis was to investigate the structure required to implement and manage digital forensic readiness within an enterprise. A comparative analysis of different digital forensic readiness frameworks was performed and, based on the findings of the analysis, the digital forensic readiness commonalities framework (DFRCF) was extended. The resultant structure was used to design a digital forensic readiness maturity assessment model (DFRMAM) that will enable organisations to assess their forensic readiness. In conclusion, both the extended DFRCF and the DFRMAM are shown to be validated by forensic practitioners, using semi-structured interviews.

A qualitative research design and methodology was used to perform a comparative analysis of the various digital forensic readiness frameworks, to comprehend the underlying structures. All the participant responses were recorded and transcribed. Analysis of the findings resulting from the study showed that participants mostly agreed with the structure of the extended DFRCF; however, key changes were introduced to the extended DFRCF. The participants also validated the DFRMAM, and the majority of respondents opted for a checklist-type MAM.

Digital forensic readiness is a very sensitive topic since organisations fear that their information might be made public and, as a result, increase their exposure to forensic incidents and reputational risk. Because of this, it was difficult to find participants who have a forensic footprint and are willing, able, and knowledgeable about digital forensic readiness.

This study will contribute to the body of knowledge by presenting an original, validated DFRCF and DFRMAM. Practitioners and organisations now have access to non-proprietary DFRMAM.

KEYWORDS and ACRONYMS

Digital Forensic Readiness (DFR); Digital Forensics Commonalities Framework (DFRCF); Maturity Assessment Model (DFRMAM); Goals and Objectives of DFR; DFR Model, Design Principles; Design Principles of Maturity Assessment Models; Digital Forensic Practitioners.

DECLARATION

I declare that “*Proposing a maturity assessment model based on the digital forensic readiness commonalities framework*" is my own work, that it has not been submitted for any degree or examination in any other university, and that all the sources I have used or quoted have been indicated and acknowledged by complete references.

Full Name: Ivan P. Claims

Signed... Date..................................

TABLE OF CONTENTS

LIST OF TABLES:

LIST OF FIGURES

CHAPTER 1: BACKGROUND

This chapter introduces the subject of digital forensic readiness, the research problem, and the subsequent research questions and research objectives. Digital forensics is the application of scientific methods to collect, identify, store, analyse, interpret, and report on digital evidence harvested from digital paraphernalia, so as to enable the recreation of illegal events as well as to anticipate prohibited actions that are disruptive to business services (Palmer, 2001).

Digital forensic readiness (DFR) is an anticipatory approach that seeks to maximise an organisation's ability to collect digital evidence whilst minimising the cost of such an operation (Danielsson & Tjostheim, 2004; Rowlingson, 2004; Tan, 2001). A particular structure is required to manage and implement DFR in an organisation.

A DFR framework can be considered as a supporting structure to implement and manage DFR (Kohn, Eloff, & Olivier, 2006). Apart from all the legislative imperatives for the need of DFR, it is also prudent to invest in the anticipatory approach to reduce the financial risks associated with cybercrime (Richardson, 2005; Whyte & Claims, 2012).

It is evident from preliminary interviews with financial services companies that organisations are dependent on digital forensics experts to develop the structure for DFR. This structure is needed to understand the scope and costs of a DFR implementation. The interviewed companies also stressed the need for an assessment model that will aid in understanding progress towards optimal DFR. The research question: "*What DFR structure (elements or domains) is needed by financial services businesses and how can such a structure contribute to the design of a maturity assessment model that satisfies the goals and objectives of DFR?"* is thus relevant, consistent, and appropriate in the current digital forensics environment.

Background to Research Problem

Financial services companies are losing millions of rands every year as a result of cybercrime, illegal activities, and infringement of company policies. In the 6th PricewaterhouseCoopers (PWC) Global Economic Crime Survey, it emerged that cybercrime is the fourth most common crime globally and South African respondents felt that the risk of cybercrime has increased since 2010 (PWC, 2011). Cybercrime is a financial offence that is committed with the use of the internet and a computer (PWC, 2011).

An organisation or a government must improve its means to prevent corruption if it wants to achieve its economic and social objectives (Grobler, Louwrens, & Von Solms, 2010a). Organisations have a responsibility towards their shareholders and employees to prevent or mitigate the risk of economic crime and to investigate instances of cybercrime and company policy abuse. A consequence of these breaches can be the negative impact on employee morale and the organisation's reputational loss. However, organisations that do not have legally-endorsed means of investigating and building evidence for cases and presenting them in a court of law will not be able to comply.

Digital Forensic Readiness (DFR) is an anticipatory methodology that facilitates the logging of transactions, building of evidence-based cases and the secure storage of cases so that they can be presented in a court of law without any additional investigation or with minimum further investigation. Literature published on the topic suggests that Digital Forensic Readiness (DFR) improves the chances of a successful litigation (Rowlingson, 2004).

Forensic readiness facilitates the development of the security strategy for the company (Pangalos, Ilioudis, & Pagkalos, 2010). Whilst minimising the impact of security incidents, it also serves as a means to illustrate that due diligence was taken regarding information assets.

Forensic readiness is, and is becoming even more, a significant part of the Information Security Best Practices (Pangalos, Ilioudis, & Pagkalos, 2010).

Digital Forensic Readiness (DFR) can be implemented employing the following approaches:

- *Industry best-practice and standards* (for example, King III, SOX, Companies Act, ISO standards, and so forth). The majority of companies build security architectures that are based on current best practices (Pangalos et al., 2010). However, these best practices do not sufficiently consider the importance of developing procedures and controls that will have successful investigation outcomes. Thus, the necessity exists to extend existing information security best practices to contain aspects of digital forensic readiness (Pangalos et al., 2010). Companies also have to consult organisations operating in the computer forensics and risk businesses or accounting firms such as the Big 4 (Ernst & Young, KPMG, Price Waterhouse Cooper, and Deloittes) to implement DFR based on best-practice. This could be costly, especially for smaller organisations or start-up companies.
- *Literature promoted frameworks* (for example, a ten-step process for forensic readiness by Rowlingson, 2004). However, frameworks are not readily available and those that are available are not associated with any maturity models.

Small organisations are more at risk for high rate and low impact incidents since their restricted financial and technical resources will most likely increase the effect on the organisation’s viability. For example, it is very difficult for a small organisation to pay an R8 million intellectual property fine for downloading movies or music from a file-sharing website (which employees are inclined to do). The start-up company is even less likely to survive this infringement.

Barske, Stander, and Jordaan (2010) stated that companies usually suffer financially as a result of write-offs of unrecoverable losses because of lack of evidence or lack of financial freedom to obtain external consultants. The impact of such a write-off can be devastating to a small or start-up organisation.

An organisation with existing digital forensic readiness should be able to measure the level of maturity of its DFR, and an organisation without digital forensic readiness should be able to assess its level of need.

An organisation that cannot assess the level of maturity of its DFR is running the risk of losing control over it. Although aimed at project management, this view is supported by an article titled: “You cannot manage what you don’t measure” (Ramirez, 2002). The King III report recommends the assessment of all controls within an organisation and the documentation of such results (Grobler et al., 2010a). However,

- Digital Forensic Readiness (DFR) maturity assessment models are not readily available through literature.
- Consultancy firms can manage assessments, but the assessments are usually based on security risks and these assessments are not particular to DFR. Preliminary telephonic interviews and e-mail communications by the researcher of this study with consultancy firms such as PricewaterhouseCoopers, Deloittes, and KPMG indicated that some consultancies do not possess DFR assessments models, some complete these assessments as part of security risk assessment, and others use holistic approaches that focus on business processes and not on digital forensic readiness, which is akin to buying the dairy to obtain a litre of milk. This could be costly, especially for small or start-up organisations.
- A Digital Forensic Readiness (DFR) maturity assessment model should endeavour to meet the goals and objectives of DFR. In other words the assessment model and DFR

framework should align to the goals and objectives of DFR. Organisations spend vast resources in their endeavour to align the one or other entity (or activity) with another entity (or activity). The overall alignment model is an example of a model that seeks to align information technology with business strategy (Henderson & Venkatraman, 1993). A similar model was presented by Luftman et al, and called the strategic alignment model (Luftman, Lewis, & Oldach, 1993). It is reasonable to conclude that the misalignment of entities that should be aligned has undesired effects on a business, hence, the resources used and the efforts made by organisations to align these activities, post implementation. It would therefore be preferable to develop a DFR framework that is aligned with the objectives and goals of DFR. Also note that, the assessment model that will be developed by this study will be aligned because it will be derived from an aligned (DFRCF) framework. These goals are discussed in Chapter 2 of this study.

In summary, there is an increased risk for forensic incidents because of a lack of DFR assessments. Companies can consult external risk firms to perform assessments, but the costs can be considerable for small organisations. The absence of non-proprietary maturity assessment models exacerbates the problem as it means that small organisations are forced to employ costly assessment models, based on security best practice, that are not necessarily focused on DFR. This study aims to extend the DFR commonalities framework to develop a DFR maturity assessment model for financial services organisations.

Statement of the Research Problem

Financial services organisations that do not have a means to assess their digital forensic readiness increase their exposure to forensic incidents, furthermore, organisations that do perform DFR assessments, utilise frameworks that do not exclusively satisfy the goals and objectives of DFR.

Research Question

In accordance with the identified problem, the main research question is established as

> *What DFR structure (elements or domains) is needed by financial services businesses and how can such a structure contribute to the design of a maturity assessment model that satisfies the goals and objectives of DFR?*

Research Sub-Questions

Based on the research question, the research sub-questions are formulated as

- What are the objectives and goals of DFR?
- Which frameworks are used to implement DFR and what are the domains of a DFR framework?
- Which maturity assessment model can be used to assess DFR?
- What principles must be considered in the design of a DFR maturity assessment model?

Research Objectives

The following are the research objectives for this study:

- To investigate the goals and objectives of DFR.
- To investigate the DFR frameworks and their domains.
- Determine which maturity assessment models can be utilised to assess DFR.
- Determine the design principles of a maturity assessment model.

Contribution of the Research

Practical Contributions:

- Financial services companies will have a verified/validated DFR framework that will assist them to understand the scope of digital forensic readiness.
- Financial services companies and digital forensic specialists will have a verified/validated maturity assessment model that will enable them to assess their forensic maturity.

Academic Contributions:

This study contributes to the body of knowledge of digital forensics by presenting findings that illustrate the comparative results of various DFR frameworks,

This chapter introduced the research problem and explicated the significance of the problem. The chapter concluded by listing the research sub-questions, research objectives, and the contribution this study will have for academia, researchers, and practitioners. In the next chapter, a review of the literature that has been published on the topic is offered to assist in understanding how the research problem can be addressed.

CHAPTER 2: LITERATURE REVIEW

This chapter is three-fold. The first four sections of this chapter are devoted to investigating the objectives and goals of DFR, followed by an overview of available DFR frameworks. The next two sections present the comparative analysis of two frameworks and the findings thereof. The remainder of the chapter provides a discussion of the principles and objectives of maturity models, their application as DFR maturity assessment models, and the maturity model design principles.

The Objectives and Goals of Digital Forensic Readiness

Historical Overview of the Origins of DFR.

The concept of forensic readiness was first introduced by Tan (2001) in his article titled "*Forensic Readiness*". Tan (2001) recorded the objective of forensic readiness as the ability to capitalise on the usefulness of incidence evidence, whilst minimising the costs associated with an incident investigation. This concept was driven by a necessity to establish the feasibility of an incident investigation and the need to reduce the time of an investigation. In this article, Tan (2001) does not differentiate between (a) a definition of DFR (meaning of DFR) and (b) the objectives (what it aims to achieve) of DFR. In fact, the author does not define forensic readiness but chooses to focus on the objectives. These objectives are then regarded and used interchangeably as both the definition for DFR and the objectives of DFR.

In 2004, Rowlingson expanded on the concept of DFR by advocating the need to collect credible evidence (Rowlingson, 2004). It is not merely sufficient to collect evidence for the sake of it, but the evidence must withstand the scrutiny of a litigation process in the event of a forensic transgression (Grobler, Louwrens, & Von Solms, 2010b). Pro-active digital forensics was introduced into the forensic readiness domain by Bradford in 2004. Bradford et al. postulated that all preventative security measures that must be taken by a computer system must form part of DFR (Bradford, Brown, Perdue, & Self, 2004). Their article proposed that forensics should not just be aimed at data changes but also be aimed at identifying the behavioural changes of the computer user[1]. The objective of this approach is to create sufficient data to enable forensic investigators to gain a better understanding of the issues and behaviours of perpetrators.

The concept of DFR was further extended in 2010 by Grobler et al. (2010b) by ensuring that the IT and information security governance programmes are incorporated in DFR. This concept aimed to enhance governance programmes by assessing the effectiveness of controls. Their article postulated that the controls that measure the IT and information security governance must be guided by best practices such as Sarbanes-Oxley and King III. Sarbanes-Oxley (SOX) is an Act (promulgated in the USA in 2002 after the collapse of Enron) designed to ensure accuracy, reliability, and transparency in corporate disclosure, and the King Report on Governance for South Africa 2009 (King III) is a code of corporate governance for South Africa (Saica, 2013; SOX, 2013).

However, as with previous authors such as Tan (2001) and Rowlingson (2004), who only briefly mention the governance and best practice aspects, Grobler et al. (2010b) also only provide a brief overview. Proper in-depth discussions and applicability of various organisational governance and best practices are not presented in their study. However, their study emphasised the use of DF tools to improve the efficiency and effectiveness of IT and information security performance of an organisation.

Grobler et al. (2010b) also extend the definition of digital forensics (and by association, the objectives) from maximising the potential to use digital evidence to maximising the

[1] The user in the context of this research is classified as a human being who operates a computer device.

potential to use comprehensive *digital* evidence (CDE)[2]. Effectively, CDE better describes what Rowlingson (2004) proposed with "credible" evidence, in the sense that it outlines key requirements that must be sought in the process of collecting evidence. The following requirements must be met by a forensic readiness evidence collection process: (a) evidence has to link the attacker to the incident, (b) evidence must be relevant and sufficient for root cause analysis, (c) evidence must bear prosecuting weight in a court of law and (d) evidence must lead to a positive prosecution of the transgressor.

In another study by Grobler et al. (2010a), the authors conclude that literature existing up to then does not adequately consider the utilisation of DF tools in the enhancement of organisational structures. Existing literature also fails to properly define and investigate "live[3]" forensics.

Pangalos Ilioudis, and Pagkalos (2010) advocated the need to extend the range of forensics to envelop the entire information security domain. The idea is to apply forensic readiness to all auditing, monitoring, and investigatory activities. The need for forensic readiness to engulf information security is because forensics are, to date, only applied to less than 30% of business security incidents. This means that the bulk of cases do not end up in court. Nevertheless, the contravention of the corporate security policy (in all cases) with or without legal implications should still be investigated. The figure of 30% is based on a survey compiled by the Computer Security Institute (CSI) in 2007 for US-based organisations that are members of CSI.

[2] Grobler et al. (2010a) define CDE as "digital evidence that will have evidentiary weight in a court of law and that contains all the evidence necessary (relevant and sufficient) to determine the root-cause of the incident, link the attacker to the incident and will result in a successful prosecution of the perpetrator".

[3] "Live" is also called "real" time and it is the ability to capture evidence when a system is active (Grobler et al., 2010a).

In this study, the objectives and goals of digital forensic readiness, as derived from the relevant literature consulted, are summarised in Table 1:

Table 1

Goals and Objectives of DFR

No	Goals and objectives of digital forensic readiness	Reference
1	To maximise an environment's (processes, procedures, technologies) ability to harvest credible evidence.	Tan, 2001; Grobler et al., 2010b
2	To maximise the potential to use comprehensive digital evidence.	Grobler et al., 2010a; Grobler et al., 2010b
3	To minimise the cost of forensics during an incident response.	Tan, 2001
4	To gather evidence targeting the potential crimes and disputes that may adversely impact an organisation.	Rowlingson, 2004
5	To prevent anti-forensic activities.	Grobler, et al., 2010a; Grobler, et al., 2010b
6	To enhance the performance of IT & Info sec with DF tools in an organisation.	Grobler et al., 2010a; Grobler et al., 2010b
7	To demonstrate good governance by assessing the effectiveness of controls.	Grobler et al., 2010a; Grobler et al., 2010b
8	To create proper data for good investigation leads.	Bradford et al., 2004
9	To gather admissible evidence legally and without interfering with business processes.	Pangalos et al., 2010
10	To allow an investigation to proceed at a cost in proportion to the incident.	Pangalos et al., 2010
11	To minimise interruption to the business from any investigation.	Pangalos, et al., 2010
12	To ensure that evidence makes a positive impact on the outcome of any legal action.	Pangalos et al., 2010

(Source: Author)

The Frameworks for Implementation and Management of DFR

There are several digital forensic readiness frameworks; however, because of the distinct focus of this study, only six DFR frameworks met the criteria for this study. The criteria used for inclusion are as follow:

- The framework must be part of academic literature.
- The framework must be applicable to computer or digital forensics.
- The framework must focus on digital forensic *readiness*.

The six frameworks that met these criteria are shown in Table 2, below:

Table 2

Digital Forensic Readiness frameworks

Literature	Framework	Research approach	Reference
The need for a structured approach to digital forensic readiness	The structured approach	No explicit approach was indicated in the article, however the study implies that a qualitative approach was followed to understand the DFR needs of an organisation	Danielsson & Tjostheim, 2004
A Ten Step Process for Forensic Readiness	The ten-step process	No explicit approach was indicated in the article, however the study implies that a qualitative approach was followed to understand the DFR needs of an organisation	Rowlingson, 2004
A Digital Forensic Readiness Framework for South African SME's	Untitled (It will be named the Barske, et al framework for the purposes of this research)	No explicit approach was indicated in the article, however a thematic analysis was performed to categorise DFR aspects, this type of analysis is indicative of a qualitative approach	Barske et al., 2010
A Framework to Guide the Implementation of Proactive Digital Forensics in Organisations	The DF Management Framework (DFMF)	No explicit approach was indicated in the article, however the study seeks answers to the questions of "why, how, when, where, what and who". This paper argues that a qualitative approach was utilised to answer these types of questions especially since the answers were descriptive and rich.	Grobler et al., 2010a
Towards a Digital Forensic Readiness Framework for Public Key Infrastructure Systems	Public Key Infrastructure (PKI)	No explicit approach was indicated in the article, however the study implies that a qualitative approach was followed to understand the DFR needs of an organisation	Valjarevic & Venter, 2011
The State of Forensic Readiness of Financial Services Companies in South Africa	DFR commonalities framework (DFRCF)	A mixed method was utilised in this study.	Whyte & Claims, 2012

Further examination of the frameworks revealed that

- The structured approach and the ten-step process frameworks were already investigated and incorporated in the *DFR commonalities framework* (Whyte & Claims, 2012). These two frameworks were thus excluded from this study as the DFRCF already harnessed the best of both. It is sufficient to note, in summary, that the structured approach

    1. excludes DFR training from its approach
    2. does not have an incident escalation policy
    3. does not have guidelines, policies, and procedures for evidence management,
    4. and does not consider awareness around DFR policies and the penalties for non-compliance.

  On the other hand, the ten-step process

    1. excludes the methodology for evidence collection and storage,
    2. does not consider the criteria for incident reporting nor does it propose a standard for stakeholder engagement during incident investigations,
    3. does not have guidelines, policies, and procedures for evidence management,
    4. and does not consider awareness around DFR policies and the penalties for non-compliance.

- The Barske et al. (2010) framework is similar to the DFRCF because both studies examined and incorporated findings as described in the unpublished article: "*The case for digital forensic readiness*" (Jordaan, 2009). This study will exclude the Barske et al. framework for the above reason and because the Barske et al. framework is limited in scope, compared to the DFRCF that investigated three frameworks in total, whereas the Barske et al. (2010) framework investigated only one framework.

- The Public Key Infrastructure (PKI) framework is designed specifically for digital certificates and message encryption and it aims to improve the information system security of a PKI system. This study does not have the above focus and thus the PKI framework will be excluded from this study.

Because of the exclusion of the above frameworks, only the DFRCF and the DFMF frameworks will be investigated in this study. An overview of the DFRCF and DFMF frameworks follows, as well as a comparative analysis that initiates the extension of the DFRCF.

Digital Forensics Readiness Commonalities Framework (DFRCF)

Figure 1 below illustrates the major domains of the DFRCF and their interrelationships. The arrows indicate a flow or steps that guide the development and implementation of DFR in organisations. Typically, organisations need to articulate their DFR strategy, which, in turn, informs the forensic-need methodology. The next step ensures the identification of systems and events that house the forensic evidence. Policies to guide the data collection and compliance will be developed after systems have been identified. Staff will have to be trained to manage forensic evidence and this step leads to the development of monitoring reports and protocol. As can be seen, the framework advocates the utilisation and approval of legal experts throughout the entire process.

It is clear from the above brief description that the domains are interlinked and each has to be acted on to ensure a holistic approach.

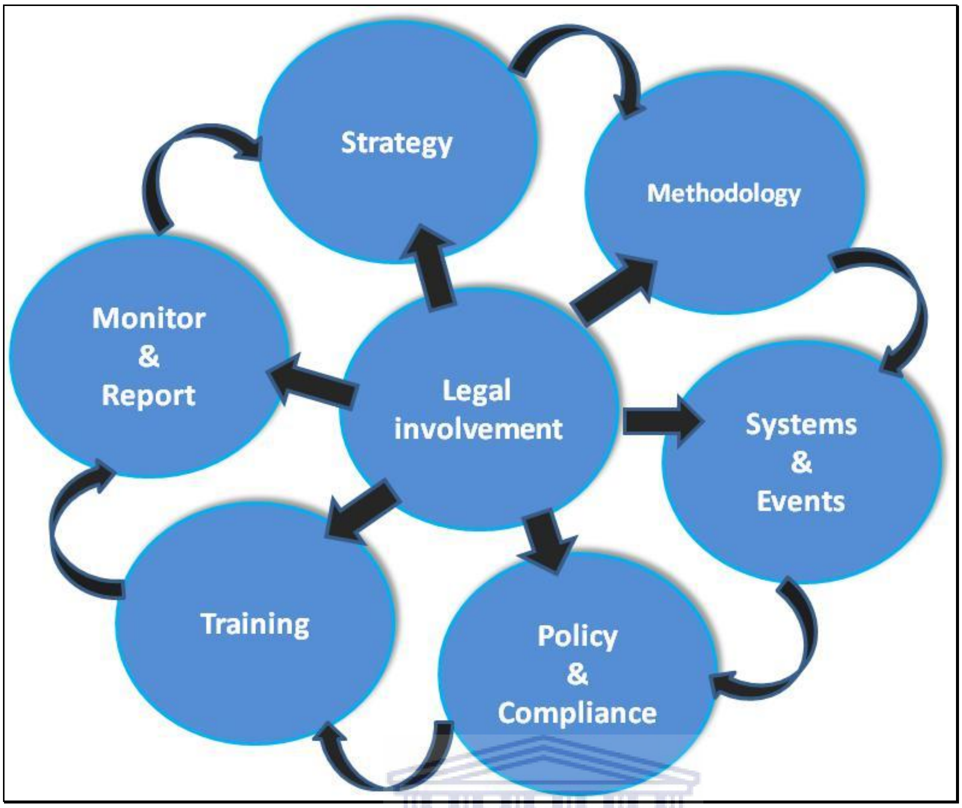


Figure 1**: DFR Commonalities framework (Source: Whyte & Claims, 2012)**

In the following section, the domains of the DFRC framework are delineated:

Strategy

The purpose of this domain is to ensure that the organisation has a DFR strategy and that it has constructed a technique to evaluate the need for evidence collection.

This Digital Forensic Readiness Commonalities Framework (DFRCF) domain is also supported in the reviewed literature. The domain emphasises the need for a strategic mandate from executive management to implement and maintain digital forensic readiness (Grobler et al., 2010a). A strategy communicated from this level will ensure top management commitment and will promote the DFR framework downwards. It also ensures that resources and finances are allocated to facilitate DFR.

The framework suggests that the implementation of this particular domain can assist with the realisation of a DF strategy and an evidence-collection statement to enable the alignment of business risk units with incident-monitoring units (Whyte & Claims, 2012)

Methodology

The purpose of this domain is to ensure the selection of a methodology that will enable the collection of comprehensive evidence as well as develop guidelines that will facilitate the secure storage and handling of evidence for cases (Jordaan, 2009). This methodology will inform the techniques that can be employed to collect, store, investigate, and report security incidents. As organisations are different and have different evidence-collection needs, the methodology that is selected should be a best fit for that particular organisation.

Legal involvement

The legal resources of an organisation must be consulted to ensure that their requirements on the subject of legislation, compliance, and limitations to collecting and storing comprehensive digital evidence are considered (Jordaan, 2009). The legal resources must be consulted for matters concerning policies, procedures, documentation, and reports (Rowlingson, 2004).

Legal advisors must be trained and experienced in cyber laws and admissibility of such evidence, especially since such evidence might span several jurisdictions, for example, from South Africa to the UK (Rowlingson, 2004; Whyte & Claims, 2012).

Systems and events

The purpose of this domain is to identify all the source systems (hardware, software, technologies, people, policies, and procedures) that might house potential evidence, so that they may be included in the DFR strategy (Danielsson & Tjostheim, 2004). It also ensures that business events and processes that necessitate digital evidence are identified. This is essentially a risk assessment that is conducted at business level (Rowlingson, 2004). Below are a few examples of systems and technologies that might house potential evidence:

- Phone logs
- Firewalls

- Monitoring software
- Routers
- CCTV cameras
- Computers

Training

Personnel and stakeholders must be suitably trained to handle potential evidence (Jordaan, 2009; Valjarevic & Venter, 2011). Staff (especially those responding to incidents) that are not properly trained can negatively affect the results of a forensic investigation as there is a risk of them polluting the evidence (Rowlingson, 2004). Listed below are a few examples of groups that must undergo training:

- Systems administrators
- Human resource departments
- Legal advisors
- IT managers
- Investigating teams
- Process owners

Monitor and report

Sources that house potential evidence must be monitored to detect threats. Intrusion detection systems (IDS) are configured to report events when predefined threats are triggered and content checkers are triggered by certain keywords (Rowlingson, 2004). The suspicious event must be investigated and a decision must be made when and how to deal with the incident. The purpose of this step is to understand which IDS must be acquired, how they need to function, how triggers must respond, in what format a response should be, when to escalate to the next level, reporting criteria, and the standardisation of interaction between concerned parties (Danielsson & Tjostheim, 2004).

Policy and compliance

This step ensures that evidence collection, storage, and handling policies and guidelines are in place. This step also allows producing a policy guideline on how a comprehensive evidence-based case must be built. Law and regulatory compliance is sought and incorporated in the security and IT policies. Some incidents are reportable under a compliance regime (Danielsson & Tjostheim, 2004):

- Employees and stakeholders should be aware of the policies and procedures.
- Compliance to these policies must be advocated.
- The consequences for non-compliance must also be well documented.
- Policies must be reviewed as must their review frequencies.

Digital Forensics Management Framework (DFMF)

A management framework for digital forensics was proposed by Grobler et al. (2010a). Their framework for proactive forensics is shown in Figure 2. As mentioned earlier, proactive forensics is a synonym for digital forensics.

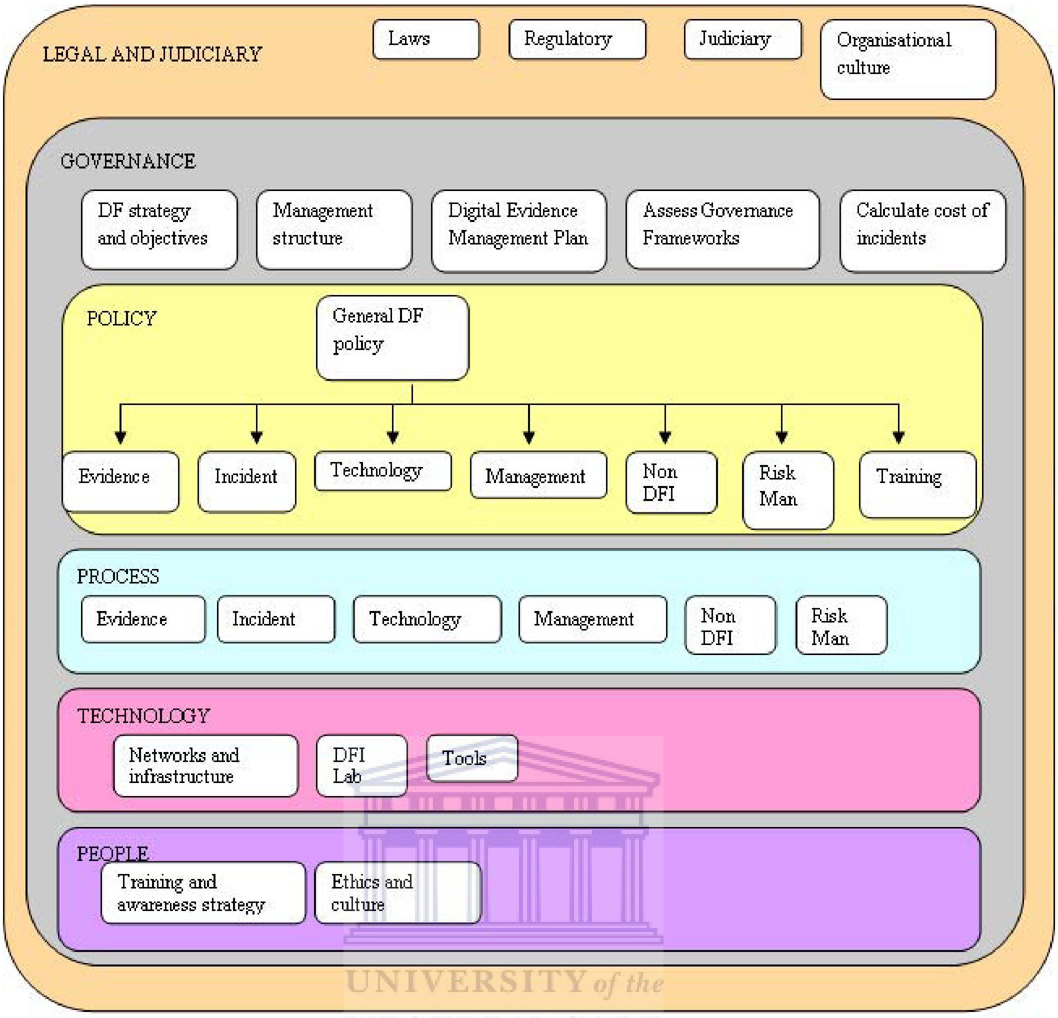


***Figure 2*: DFMF and its elements (Source: Grobler et al., 2010a).**

Legal and judicial

This domain deals with compliance and responds to the question “why”? The origin or purpose of this question is not clear but one can assume it relates to and answers the question: “Why is DFR required?” This domain refers to the judicial, regulatory, and legal requirements that will enable the implementation of DF in the organisation. The judicial requirements for countries might be different; for this reason, the requirements must be determined (Casey, 2004). For instance, does the HMG Security Policy Framework (SPF) principle apply for the processes of securing information? If the company operates within the UK’s government domain, then it does.

Grobler et al. (2010a) implied that the implementation of this step can foster the understanding of (a) court requirements, (b) regulatory requirements, (c) organisational culture, and (d) bylaws.

Governance

This domain also deals with the question “why?” It takes into account corporate governance as well as strategic, tactical, and operational management requirements. This deals with risk management in the organisation and also with the management of stakeholders and facilities. Companies must prepare a DF strategy with objectives and it must be included in the organisational structure (Grobler et al., 2010a; Grobler et al., 2010b).

In the article by Grobler et al. (2010a), they maintain that possible outcomes from implementing this step would be the following:

- A DF strategy with strategic goals,
- An evidence control plan,
- An assessment of governance controls, and
- A framework to estimate costs of incidents.

Policy

The questions “what?”, “when?” and “who?” can be answered within this domain. Organisations must own a DF policy framework in which resides a general DF policy with auxiliary sub-policies (Grobler et al., 2010a; Grobler et al., 2010b). The general policy should provide an overview of the application and strategic intent. The sub-policies should provide detailed information evidence management and should include things such as evidence handling, evidence storing, and so forth.

In their article, Grobler et al. (2010a) imply that possible outcomes from implementing this step can be the formation of

- A DF policy framework, and

- Sub-policies within the general DF policy.

Process

The process domain supports the policy domain that provides guidance on implementation of policies and procedure. Procedures and processes must be forensically sound, as defined by Louwrens et al. (2006, p. 680) “processes that maintain the integrity of evidence, ensuring that the chain of custody remains unbroken and that collected evidence will be admissible in a court of law”.

Grobler et al. (2010a) claimed that possible outcomes from implementing this step can be the development of

- process guidelines,
- procedures, and
- processes that will support the Policy domain.

Technology

No organisation can do proper incidence investigation without DF tools and techniques; thus, this element addresses technologies and applications to use (Grobler et al., 2010a). Various DF tools can be used in different situations, for example, key-stroke loggers, write blockers, and EnCase—which is investigative software. A DF investigation laboratory is also advised (Grobler et al., 2010a).

In their article, Grobler et al. (2010a) observed that possible outcomes from implementing this step can be

- A well-equipped laboratory that houses DF tools and technologies;
- A network infrastructure to support the DF strategy.

People

A DF training strategy and awareness programmes must be in place and should concentrate on the needs of different users. The findings of this study indicate that a possible outcome from implementing this step can be the development of a training and awareness strategy with accredited training programmes.

Comparison of DFRCF and DFMF:

The two frameworks extend one another and are largely similar apart from the obvious difference in terms of graphical presentation. The DFMF is displayed as a flat, layered box, which makes the underlying sub-domains visible. This ensures transparency and provides information at a glance. The DFRCF is displayed as a cycling wheel with the Legal domain as the axis—similar to a continuous process improvement model based on the Deming cycle. The cycling wheel indicates the continuous progress towards optimal forensic readiness.

The key difference between the two frameworks is their focal points. The DFMF is aimed at managing existing DFR, whereas the DFRCF is a framework for implementation of DFR.

Obvious similarities

The obvious similarities of the two frameworks are illustrated in Table 3 below. The table highlights the naming convention that used in the two frameworks.

Table 3

Obvious Similarities of the Two Frameworks

Legal element	
Element Name	Framework
Legal involvement	DFRCF
Legal & Judicial	DFMF

(Source: Author)

The above table suggests that this study must consider the legal, judicial, and legislative requirements of the country(ies) within which the organisation does business. Expert legal advice must be sought to elicit and understand the requirements (Casey, 2004).

Obscured similarities

The concept of the People domain in the DFMF is misleading, because although the implied focus is on people, it goes on to discuss the training needs and the importance of accredited training and awareness programmes. The DFRCF named this domain the Training domain because, after all, the intended maturity model will assess the availability and penetration of training and awareness programmes. Both the frameworks have a Policy domain; however, the DFRCF has combined the Policy domain with the Compliance domain. Both of these domains are (a) major elements within DFR, and (b) address separate topics (Compliance advocates conformity to legislation and the Policy domain highlights the required documentation to be developed for DFR). It is clear from the above that the two domains warrant being discussed and presented as separate and different concepts and not as a single concept, as done by the DFRCF. In this study, the Policy domain is presented independently from the Compliance domain for the above reasons.

The Systems and Events domain of the DFRCF is similar to the Technology and the Process elements of the DFMF. The DFRC framework combined the technology and process aspects of DFR within their System and Events domain because an information system can includes facets such as technologies, applications, hardware, manual inputs, and processes.

Rowlingson (2004) further suggested that the identification and classification of hardware, software, processes, and events (that house potential digital evidence) should be performed as part of an activity within the Systems and Events domain. I, the researcher in this study, found it appropriate to retain the Systems and Events domain, as suggested by the DFRCF. Although Information systems and Events would be a better description for this domain, this study chose the shortened version, that is, Systems and Events, to keep the domain names succinct.

The DFRCF created a separate Methodology element that is tasked with investigating the evidence-collection needs of an organisation. The expected outcome of this element is an evidence-collection methodology and techniques for evidence management. The DFMF included the evidence-collection methodology and techniques in the Strategy element. This is practical, and it makes sense to do so, as the establishment of a methodology is also a strategic mandate. The DFRCF should consider including the methodology within the Strategy.

Disparities

The DFMF and the DFRCF applied different approaches to the Governance domain. The DFMF created the Governance element based on the goal of "proving (assessing) the effectiveness of controls, measured against IT and information security objectives" (Grobler et al., 2010a, p. 682). This implies that compliance and governance is used synonymously or that governance is an umbrella term that includes compliance.

This study recognised the need to separate governance from compliance, because governance is considered to be the mechanisms, capabilities, and decision structures that must be put in place to ensure compliance to procedures, policies, and legislations within an organisation (Bonazzi, Hussami & Pigneur, 2010; Brown et al., 2006). On the other hand, compliance is considered to be the act of adhering or the act of demonstrating conformance to procedures, policies, and legislations within an organisation (Bonanzzi et al., 2010).

The term *compliance* is more appropriate for the action of: "proving (assessing) the effectiveness of controls, measured against IT and information security objectives" (Grobler et al., 2010a, p.682). It means that DFMF can consider separating Governance from Compliance and creating two separate major domains that each focuses on the different aspects mentioned.

Although the Strategy and Compliance domains of the DFRCF and the Governance domain of the DFMF look similar, their focus differs: the focus of DFRCF is the compliance of policies, guidelines, objectives, and systems to DFR, whereas the DFMF focuses on the governance (and compliance) of policies, procedures, technology, and people.

Consequently, the DFRCF should be extended to include a Governance domain as described by the DFMF. On the other hand, the DFMF could consider separating compliance from governance as these two aspects have different focuses.

The designer of a framework has to consider the monitoring of systems or sources that house potential evidence, to detect threats (Valjarevic & Venter, 2011). The purpose of the Monitoring and Reporting domain is to identify the system's requirements and their function, event triggers and their response requirements, response formats, and the reporting criteria (Danielsson & Tjostheim, 2004). At this stage, the organisation would also want to specify when the event can be escalated and what the protocol for interaction between concerned parties must be (Jordaan, 2009; Rowlingson, 2004).

Of the two frameworks examined, only the DFRCF considers the above requirement. The DFMF should consider incorporating a domain that focuses on the monitoring of source systems that enable an organisation to understand its system acquisition needs, how triggers should be managed, what form the event responses should take, and what the reporting criteria should be.

Summary of the Main Findings of the Comparative Analysis

Table 4 below provides a summarised view of the findings that emerged from the comparative analysis of the DFMF and the DFRCF. The table provides a quick view of the DFR aspects that can be changed to augment the two frameworks. The detailed discussion illustrating how the DFRCF is extended is done in Chapter 3 of this study.

Table 4

Findings of the Comparative Analysis

DFMF	DFRCF
Model is graphically presented as a flat layered box, with visible sub-domains	Model is graphically displayed as cycling wheel with the Legal domain as the axis
Is focused towards managing existing DFR	Is focused on the implementation of DFR
Can consider separating Governance from Compliance	Can consider separating Policy from Compliance
The domain titled: "People" is misleading and can be properly renamed to "Training"	Can consider elaborating and describing in fuller details the activities concerned with processes within the Policy domain
Can consider including a domain that focuses on the monitoring source systems	Can consider making the methodology aspect and the development of an organisation structure part of the Strategy domain

The following sections of this chapter focus on the objectives and design principles of a maturity assessment model. It then concludes by exploring modelling approaches and proposing a DFR maturity matrix.

Principles and Objectives of a Maturity Model

An assessment can be defined as the procedure of evaluating an entity against a model for continuous improvement so that the entity can realise what has been accomplished and what needs to be improved (Hillman, 1994). Hillman further reiterated the importance of selecting a suitable framework that is widely adopted to ensure comparisons against peers. The lack of existing DFR maturity models make this objective impossible to achieve.

The following are some of the objectives and goals of maturity assessment models:

- To discover areas needing improvement and to act on them and to maintain what has been performed well.
- To help in directing organisations in the designing of processes that lead to a "state of maturity in the area for which the model was developed" (White, 2007, p. 2).
- To assess the maturity of the procedure and to assign a maturity level.

- To match up to the maturity of the organisation’s process against other organisations and against best-practices.
- To present a method of learning to enhance the maturity level (Randeree, Mahal, & Narwani, 2012).

Maturity Models to Assess DFR

As mentioned earlier in the study, organisations integrate DFR in the information security domain and also assess it as part of the information security domain. The problem with this approach is that information security neglects the magnitude of developing procedures and controls that will have successful investigation outcomes (Pangalos et al., 2010: p. 16). This means that the assessment of DFR as part of information security is discouraged because this approach will lead to a failure to satisfy the DFR objective that seeks to “demonstrate good governance by assessing the effectiveness of controls”.

Moreover, forensics is applied to less than 30% of business security incidents (Pangalos et al., 2010). This implies that the DFR assessments that are performed as part of the information security are potentially based on a small percentage of security incidents. Such an assessment will present a dubious view of the state of DFR.

An added complexity is the disparate focal points of Information security and DFR. Information security focuses on the availability, reliability, and confidentiality of information, whereas digital forensic readiness is concerned with the identification, preservation, analyses, and presentation of information (Pangalos & Katos, 2010). It is thus conceivable that an information security assessment will not have a DFR focus.

Furthermore, traditional security models struggle with the alignment of IT security and the strategic business objectives (Grandison, Bilger, O’Connor, Graf, Swimmer, Schunter, Wespi, & Zunic, 2007). DFR requires an alignment between the business and legal requirements as well as the IT strategy, as is evident in the Strategy domain of the DFRC framework. Thus, it would not be advisable to apply a model that disregards the need to align IT with business objectives.

As mentioned earlier in this study; preliminary interviews with forensic practitioners and organisations that are concerned with DFR highlight the fact that their practices only assess DFR as part of information security. Thus, it seems as if this approach is considered a best practice, at least for the four reputed organisations consulted. In the course of this study, no alternative approaches[4] (academic or non-proprietary) to assess DFR were encountered.

Therefore, because of the (a) above-mentioned shortcomings in the approach to using information security assessment to assess DFR and (b) due to a lack of existing DFR maturity models, this study will develop a DFR maturity assessment model (DFRMAM) based on the structure of the extended DFRC framework. In addition to the structure of the extended DFRCF, this study will also exploit the maturity matrix that is suggested within the data-centric security model (DCSM) by incorporating it into the proposed DFRMAM.

The use of the DCSM was selected for this study because, like the DFRCF, (a) it is informed by the objectives of the business strategy and requirements, (b) it aligns IT security with business strategy, and (c) the model was designed by IBM, one of the most respected and innovative companies (*Business Week*, 2009).

The Data Centric Security Model (DCSM)

This model was designed by IBM to assist organisations to align their IT capability with their business goals (Van Cleeff, 2008). The model achieves this by directly connecting security activities to the data it protects (Grandison et al., 2007).

The model has two main components (domains), namely the policy and the data pillars (see Figure 3 below).

[4] Note: this researcher did discover one alternative approach, but only during the data collection stage, not prior to the data collection stage.

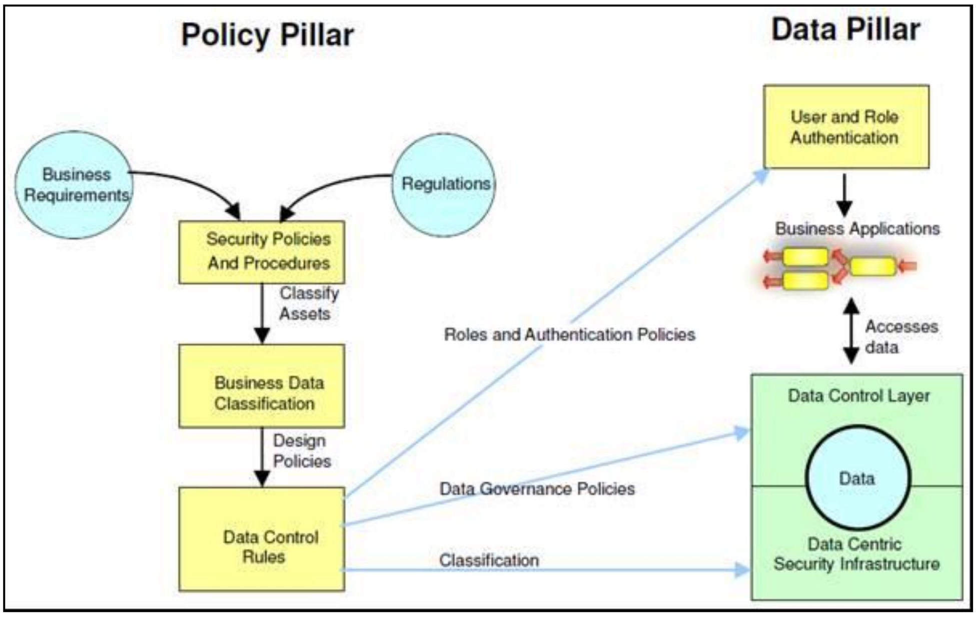


***Figure 3*: Data centric security model (Source: Van Cleeff, 2008, p. 113).**

An overview of the pillars, and the maturity matrix of the DCSM, follows next. The ensuing discussion on the pillars and maturity matrix are brief because it is not the intention in this study to utilise the pillars or their content. Only the naming convention of the maturity levels of the DCSM will be used by this study. The detail (description) of the maturity levels will be extracted from forensic practitioners during the data gathering phase of the study.

Policy pillar

The following is a summary of the activities presented within the policy pillar:

- The organisation will gather all the business and legal requirements and resolve all conflicts and document a set of cohesive requirements.
- The business and legal requirements are fed into a description for data security policies and procedures.
- Data attributes and labels are used to determine the data classes. Data are also classified by ownership, origin, time, and location, and data governance is an outcome of this step.

- The policy classification and governance are encoded into a set of data control rules. The rules determine practices for handling and accessing data.

Data pillar

The following is a summary of the activities presented within the data pillar:

- Access to data and permissible actions are controlled by a data control layer, as indicated by the data control rules.
- There are different layers of protection and access through roles, business applications, and infrastructure.

Maturity matrix of the DCSM

Table 5 below illustrates the maturity matrix of the DCSM. The maturity matrix consists of the components (sub-domains) and the adoption levels (maturity levels). What follows is a discussion on the components and the maturity levels.

Table 5

The Maturity Matrix Of The DCSM

Components	Adoption levels			
	Basic	Intermediate	Advanced	Full
Security Infrastructure				
Business Data classification				
Role Definitions				
Policies by classification				
Data is labelled				
Data Flow Analysis				
Automated policy provisioning				

(Source: Van Cleeff, 2008, p. 114)

Maturity components (sub-domains)

The following are the components (sub-domains) of the policy and the data pillars (domains).

- Security infrastructure:

  This is the first phase of the initial execution of the policy pillar, which is responsible for the identification of data types and business and legal requirements of the organisation.

- Business data classification:

  Data attributes and labels are used to determine the data classes. Data is also classified by ownership, origin, time, and location, and data governance is an outcome of this step.

- Roles definitions:

  A the top of the data pillar is a role-based authentication component that identifies users and assigns roles to the users based on authentication policies provided by the policy pillar.

- Policies by classification:

  Policy designs are federated between multiple authorities inside an enterprise.

- Data is labelled:

  This is the enabling of runtime labelling of channels and data while enabling automated policy selection.

- Data flow analysis:

  Data and communication channels are labelled at runtime.

- Automated policy provisioning:

  Systems normally have multiple policies based on the classification of the data. The policies are designed separately and then provisioned for the different system types.

Adoption levels (maturity levels)

The DCS model has four adoption (maturity) levels, namely Level 1: Basic, Level 2: Intermediate, Level 3: Advanced, and Level 4: Full (Grandison et al., 2007; Van Cleeff, 2008). Each of the levels is discussed below:

- Level 1: Basic

  This model suggests that most organisations exhibit this level of maturity because, at this stage, the organisation would have defined the information security requirements needed to protect critical information assets. This, however, may lead to overprotection of non-critical information assets. Simply put, this can be related to the DFR as at this level, an organisation needs to have a basic understanding of the forensic needs. However, this study will only utilise the naming convention, namely, Level 1: Basic. This implies that the basics of DFR are observed by organisations.

- Level 2: Intermediate

  This level will be reached when organisations have agreed on data classifications, have agreed on the protection required per classification, and security is implemented considering the most critical information assets. This is also where the organisation must demonstrate that it has policies that are designed for each system. DFRMAM can relate to this final step since the model has to assess whether the various forensic policies have been implemented within the organisation.

- Level 3: Advanced

  This level of maturity implies that an organisation has systems that can, amongst others, use an assortment of access control rules for the varied type of data it interacts with. There is no clear understanding how the description of this maturity level can be used by the DFRMAM; however, as mentioned earlier; this DFRMAM will only utilise the name of the maturity level.

- Level 4: Full

  For organisations to reach this level, they would have had to achieve all the previous ratings, as listed by the preceding maturity levels. In addition to this, the organisation would have systems that perform automated security policy management. However, it appears as if the authors Grandison et al.(2007) have not successfully managed to distinguish between Level 4 and Level 5, as it is unclear what the differentiating factor is. There is no clear understanding of how the description of this maturity level can be used by the DFRMAM.

Design Principles to Consider When Developing a Model

This section discusses the principles that must be observed throughout the development lifecycle of a maturity model and identify the model contents that need further clarification through data collection.

Authors of literature on this topic have already dealt with the aspects of design principles (De Bruin, Freeze, Kaulkarni, & Rosemann, 2005; Maier, Moultrie, & Clarkson, 2009; Becker, Knackstedt, & Pöppelbuß, 2009; Solli-Sæther & Gottschalk, 2010; Pöppelbuß & Röglinger, 2011; Röglinger, Pöppelbuß, & Becker, 2012). For this study, the design structures as proposed by two studies are employed, namely those of

- De Bruin et al. (2005), because this study is cited in several articles and thus became popular, and
- Pöppelbuß et al. (2011), because their study encapsulates different design principles to propose a practical checklist for researchers involved in the design of maturity models.

A maturity model development framework

According to De Bruin et al. (2005), a maturity model must have a development framework that considers the purpose for which the framework is designed. The maturity assessment design may be descriptive, prescriptive, or comparative.

- A descriptive model is defined as a single-point event that does not plot a path towards improving maturity or it is a model that does not present relationships to performance. This model is good for assessing the current standing of an event and it is used as a diagnostic tool (Maier et al., 2009; Pöppelbuß et al., 2011).
- A prescriptive model focuses on the emphasis of domain relationships in relation to business performance. It also plots a path to maturity.
- The comparative model allows the comparison of similar practices across industries.

It is, however, more feasible that the above models are an evolution of each other as a model can, at first, be descriptive, as it understands its immediate environment. Then it grows into the prescriptive state as it repeatedly achieves deeper understanding until it can be applied across industries.

In addition to the abovementioned three types of models, Pöppelbuß et al. (2011) postulated an additional model; the basic model. They suggested that this model is so rudimentary that its only purpose is to illustrate the minimum aspects of a model.

There is thus an evolutionary aspect in the “coming of age” of a maturity model—as depicted in Figure 4. This implies that the descriptive model must comply with the basic model’s design principle and the prescriptive model must comply with the descriptive model’s design principle, and so on.

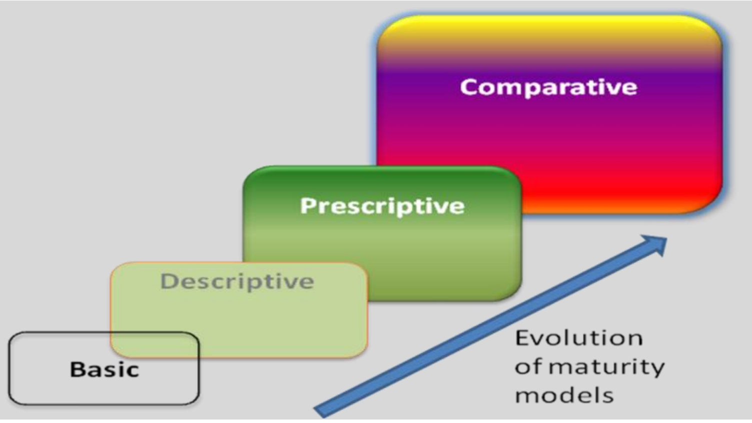


***Figure 4*: Evolution of maturity model (Source: Pöppelbuß et al., 2011).**

This study will adopt a prescriptive model design approach to baseline a model for further research and input. The natural evolution to a comparative model should happen after the model has been tested and applied and changes have been incorporated into the model. A second iteration would thus be required. This falls outside the scope of this study.

Development framework and its phases

Figure 6 below illustrates the different phases within the standard model development framework. The model can be applied across disciplines. Models such as the business process maturity models and knowledge management capability assessment were developed using the standard development model framework (De Bruin et al., 2005).

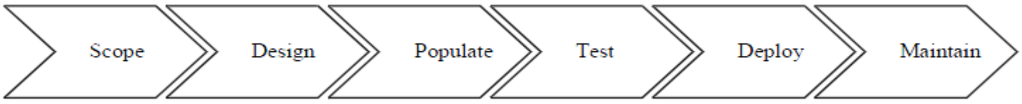


***Figure 5*: Model development framework (Source: De Brui, et al., 2005, p. 3)**

Van Steenbergen, Bos, Brinkkemper, Van de Weerd, and Bekkers (2010) proposed a similar methodology for developing focus-area maturity models, as depicted in Figure 6 below.

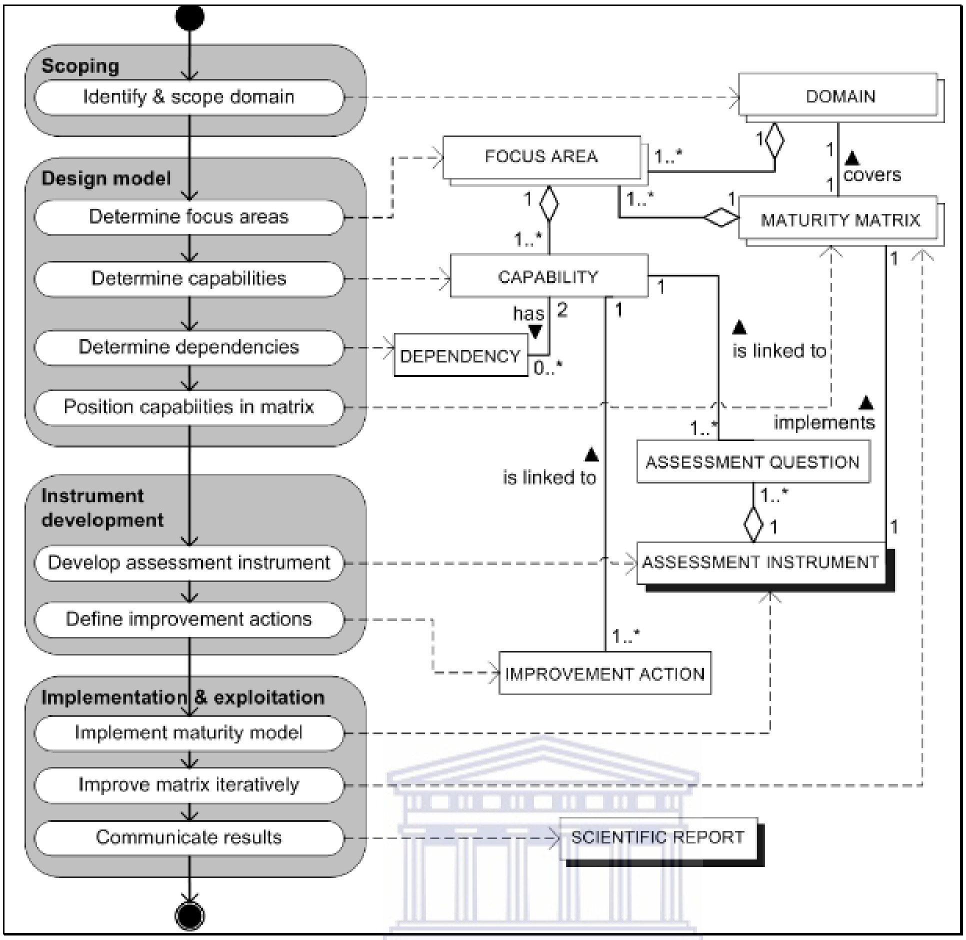


Figure 6: **Focus area maturity models (Source: Steenbergen et al., 2010).**

The focus-area maturity model has four phases, namely, scoping, design model, instrument development, and finally, the implementation and exploitation phase. Unfortunately, the model and discussions of the article do not articulate the notations within the phases. As mentioned, the models are mostly similar, with differences primarily in the naming of phases and the number of phases. Key differences between the models are as follow:

- The model development framework does not consider dependencies between elements or sub-elements. This is important to highlight so that it becomes transparent when plotting a performance plan.
- The model development framework does not have a communication plan, especially one that is as formal as the focus area maturity models. Although

this is implied within the maintenance phase, it is worthy of a mention so that it becomes part of the maintenance plan.

- The focus-area maturity model does not have a test phase. It is important to test the contents and design with a pilot study and bring about changes iteratively to achieve wide acceptance and adoption.

1. **Scoping phase**

This is the first phase of the development and it sets the boundaries for application and its use. The major decisions to be made are illustrated by Table 6 below. The checkmarks indicate the decisions applicable to this study.

Table 6

Decision Points for Maturity Model

Criterion	Characteristics			
Focus of Model	Domain specific √		General	
Prerequisites for applicability (Pöppelbuß et al., 2011)	Good understanding of digital forensic readiness.			
Purpose of use (Pöppelbuß et al., 2011)	To assist organisations to gauge their level of maturity towards forensic readiness and thereby to provide a tool to examine the gap to a state of full maturity.			
Model differentiation (Pöppelbuß et al., 2011)	There are no existing DFR models to differentiate against. This model is aimed at DFR—no other models have this focus.			
Development stakeholders	Academia	Practitioners √	Government	Combination

(Source: De Bruin, et al. 2005)

The focus of the model will be particular to digital forensic readiness, and it is aimed at practitioners with a good understanding of DFR. This focus distinguishes it from other models. Pöppelbuß et al. (2011) advocated the inclusion of pre-requisites, purpose, and differentiation as part of the aspects of designing a model and will thus be included in this model.

2. **Designing phase**

a. **Design metrics**

The second phase’s objective is to establish an architecture or design of the model. Table 7 below indicates the major decisions to be made in this phase. The checkmarks show the decisions applicable to this study.

Table 7

Decision When Designing a Maturity Model

<table>
<tr><th>Criterion</th><th colspan="3">Characteristics</th></tr>
<tr><td rowspan="2">Audience</td><td colspan="2">Internal √</td><td>External √</td></tr>
<tr><td colspan="2">Executives, Management √</td><td>Auditors, Practitioners, academics √</td></tr>
<tr><td>Method of application</td><td>Self-assessment √</td><td>Third Party Assisted√</td><td>Certified Practitioner</td></tr>
<tr><td>Driver of application</td><td>Internal requirement</td><td>External requirement</td><td>Both √</td></tr>
<tr><td>Respondents</td><td>Management √</td><td>Staff √</td><td>Business Partners</td></tr>
<tr><td>Application</td><td>1 entity/ region √</td><td>Multiple entities/single region√</td><td>Multiple entities/multiple regions √</td></tr>
</table>

(Source: De Bruin, et al. 2005)

The model is primarily aimed for internal use by executives and management, but it is envisaged that external academics (such as the author of this study) will play an initial role in the assessment of an organisation. There will be an initial external drive from academics to have the model evaluated and tested. Organisations will be able to do self-assessment and or consult academics to perform assessments. The initial drive will be external.

This will, it is hoped, change as more entities become aware of the model and its uses. The participants will be the management team and staff in critical forensic roles. This mode is aimed at organisations that will mostly be operating in a single region with a single entity. However, in this study, the model with organisations that have multiple entities and multiple regions to examine the extensibility of the model will also be tested.

b. Maturity levels

This phase determines the maturity levels and descriptions. A top-down or bottom-up approach is usually employed to establish the levels of maturity. Definitions of the maturity levels are first developed before measures are defined to fit the definitions—in a top-down approach. The bottom-up approach encourages the development of measures first and the retrofit of definitions to fit the measures (De Bruin et al., 2005).

Table 8 below identifies the major decisions to be made in the phase and the checkmarks indicate what decisions were made for this study.

Table 8

Proposed Maturity Levels and Definitions

Criterion	Characteristics	
Approach	Top-down √	Bottom-up
Maturity levels	Level 1: Non-existent	To be defined
	Level 2: Basic	To be defined
	Level 3: Intermediate	To be defined
	Level 4: Advanced	To be defined
	Level 5: Full	To be defined

(Source: Author)

A top-down approach is envisaged, and the proposed levels are Level 1: Non-existent, Level 2: Basic, Level 3: Intermediate, Level 4: Advanced, Level 5 Full. The above levels are an adaptation of the levels suggested by the DCSM. The DCSM has four levels, but the DFRMAM will have five levels of maturity. The reason for this is that the DCSM implies that every organisation will already have a basic level of information security.

However, for this study, the need to add a level preceding the basic level was recognised; this is to accommodate organisations that have not fulfilled all the activities within the basic level. This new level will be named Level 1: Non-Existent. This will be the first level of maturity towards the path of full maturity (level 5).

The levels indicate compliance towards full DFR. For example, an assessment at Level 2 means that the entity is aware of DFR but has only fulfilled the basic requirements towards DFR maturity. Although this study proposes the definitions of the maturity levels; they will be validated with forensic practitioners during the data collection phase of this study. This is consistent with a top-down design approach.

c. **Domains (or elements) and sub-domains of the model**.

Table 9 below indicates the proposed major domains and sub-domains of the maturity assessment model. The maturity levels are adapted from the IBM's data-centric security model matrix.

Table 9

Proposed DFRMAM Domains

DFRMAM Domains
DFR Strategy
Legal requirements
Governance
Systems & Events
Policy

Compliance
Training
Monitor & Report

d. **Dependencies between domains and sub-domains**.

As proposed by the focus area maturity model, the dependencies between domains and sub-domains must be identified and clarified to ensure that a performance plan that addresses the dependencies is designed (Steenbergen et al., 2010). This dependency has already been illustrated in Chapter 2.

3. **Populate phase**

This phase is the identification of *what needs to be measured* and *how this* will *be measured*. The elements within DFR are reasonably identifiable from the related literature. However, because DFR is a relatively new field and existing literature does not provide the assessment matrix, the researched literature provides theoretical models that have not necessarily been tested in the real world. The development of sub-elements requires collaboration with practitioners and fellow academics, and this will be resolved in the data collection phase of this study.

Literature promotes the use of sub-elements to extract facets that add deeper understanding, without which it will be difficult to plot improvement strategies towards maturity (De Bruin et al., 2005). The sub-elements assist in the development of questions that must be answered to fulfil a maturity requirement. The use of Delphi techniques, case studies, focus groups, and nominal techniques is recommended to extract this information (De Bruin et al., 2005).

4. **Test phase**

De Bruin et al. (2005) proposed that a maturity model's construction, including content and instruments, must be tested for reliability, validity, and generalisability. This study will have the opportunity to do so during the data collection phase. The model will be discussed with various forensic practitioners who will validate the model by providing their input and criticism. Verifying/validating the DFRMAM will attest to its significance and relevance in the DFR domain (Soni & Kodali, 2013, p, 275).

5. **Deployment phase**

   The intention of this phase is to make the model available to its stakeholders and intended audience. Authors of the literature reviewed have suggested deploying the model within the entities that assisted with the development of the model and later to other regions that were not involved with the development of the model. This study's primary focus is the deployment of the model to fellow academics through published articles and so forth.

6. **Maintain phase**

   The goal, scope, and acceptability of the model determine the resources that are responsible to maintain the model. A repository will be necessary as the model evolves from prescriptive to comparative. The model must have resources to maintain it as its continuant relevance is determined by its maintenance over time. The repository is envisaged to be this research paper, and the resources to provide upkeep of the model will be the academics that will do further research on this model or the practitioners who will utilise the model within their practices.

The author of this study hopes that fellow academics, researchers and practitioners will see the value of the model and in doing so take responsibility for the development of the model over time.

Chapter Summary

As the reviewed literature showed, there are no existing DFR maturity assessment models; this study was conducted to undertake the development of such a model. However, to develop such an assessment model, the structure (domains and sub-domains) of DFR had to be identified. During the course of the research, several frameworks that illustrate the structure of DFR were identified, and thus, the first part of the research question was resolved by this study, namely: *"What DFR structure (elements or domains) is needed by financial services businesses?* Five of the six frameworks employed a qualitative approach to understand the forensic landscape.

Furthermore, a comparative analysis between the DFRC and the DFM frameworks was performed and the findings contributed to (a) the extension of the DFRC framework and (b) the goals and objectives of DFR. Thus, the research sub-questions 1 and 2 were answered by this study.

Moreover, it became apparent that no existing DFRMAM can be utilised for this type of study so a maturity assessment model with a maturity matrix was designed, based on the development framework as postulated by De Bruin et al. and Pöppelbuß et al. (De Bruin et al., 2005; Pöppelbuß et al., 2011). This design proposes a qualitative approach to developing and implementing the maturity assessment model. The research sub-questions 3 and 4 were therefore answered by this study.

Table10 below illustrates the design principles and content of the model. The content in the table will be evaluated with practitioners.

Table 10

Design Principles to be Tested with Practitioners

Criterion	Characteristics			
Focus of Model	Domain specific √	General		
Prerequisites for applicability (Pöppelbuß et al., 2011)	Good understanding of digital forensic readiness.			
Purpose of use (Pöppelbuß et al., 2011)	To assist organisations to gauge their level of maturity towards forensic readiness and thereby to provide a tool to examine the gap to a state of full maturity.			
Model differentiation (Pöppelbuß et al., 2011)	There are no existing DFR models to differentiate against. This model is aimed at DFR—no other models have this focus.			
Development stakeholders	Academia	Practitioners √	Government	Combination
Audience	Internal √	External √		
	Executives, Management √	Auditors, Practitioners, academics √		
Method of application	Self-assessment √	Third Party Assisted√	Certified Practitioner	
Driver of application	Internal requirement	External requirement	Both √	
Respondents	Management √	Staff √	Business Partners	
Application	1 entity/1 region √	Multiple entities/single region	Multiple entities/multiple regions √	
Approach	Top-down √	Bottom-up		
Maturity levels	Level 1: Non-existent	To be defined		
	Level 2: Basic	To be defined		
	Level 3: Intermediate	To be defined		
	Level 4: Advanced	To be defined		
	Level 5: Full	To be defined		

Table 11 below depicts the proposed major domains, sub domains, and maturity levels of the DFR maturity assessment model.

Table 11

Proposed Maturity Domains and Levels

Domains	Maturity levels				
	Non- existent	Basic	Intermediate	Advanced	Full
DFR strategy					
Legal requirements					
Governance					
Systems & Events					
Policy					
Compliance					
Training					
Monitor & report					

In the following chapter, the extended framework will be discussed in detail and the new graphical presentation of the DFRCF illustrated.

CHAPTER 3: EXTENDED DFRC FRAMEWORK

This chapter provides elaboration on the extended digital forensic readiness framework by a discussion of the domains and their outputs. It also illustrates which goals and objectives are satisfied by the domains and illustrates which domains and sub-domains should be used to compile a maturity matrix.

Extended DFRC Framework

In Figure 7, there is a graphical depiction of the extended DFRCF—before forensic expert input. It depicts the major domains (for example, strategy) and expected outputs for (example, organisation structure). The *outputs* will be referred to as *sub-domains* in this study; this is to ensure that consistency is observed within the study and also because the framework that is being extended does not refer to outputs.

The graphical depiction of the DFRC framework was changed to represent a flat layer so that the sub-domains are easily visible. The extra visibility facilitates easier conversations during the data gathering phase of the study. This framework would enable organisations, particularly small and medium enterprises (SMEs), to understand the scale and scope of implementing a DFR programme.

The extended DFRCF also illustrates the major domains and their respective sub-domains that must be assessed (measured) by the DFR maturity model. This is the structure that will be used to compile a DFR maturity assessment model.

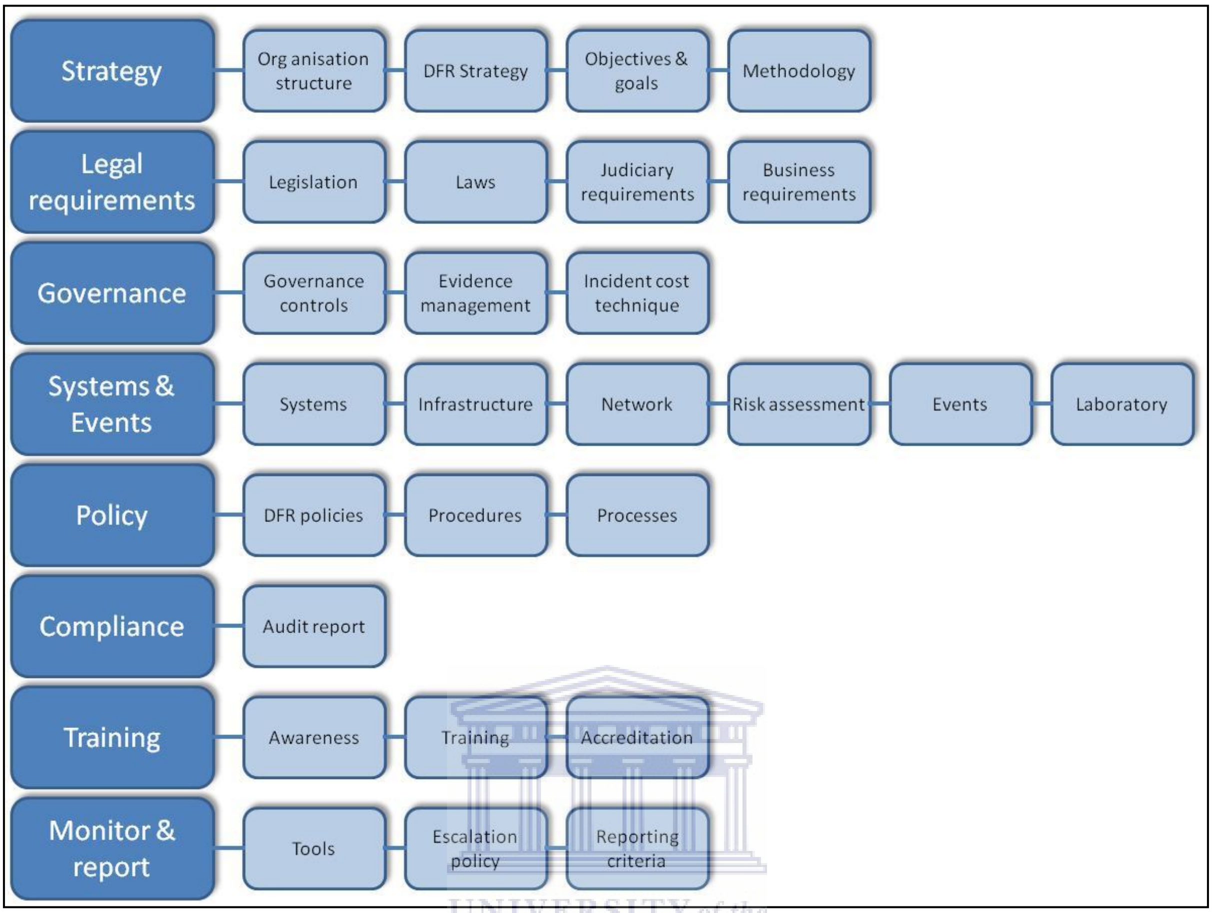


Figure 7: Extended DFRCF-v1, with domains and sub-domains, pre participant input.

The domains discussed hereafter incorporate the recommendations based on the comparative analysis that was done in Chapter 2 of this study.

Strategy

The rationale behind this domain is to ensure that an organisation has (a) a DFR strategy aligned to the organisations goals, (b) a structure that highlights the reporting lines of the forensic unit, and (c) that it has constructed a technique to evaluate the evidence collection need.

There must be a strategic mandate from executive management to implement and maintain digital forensic readiness (Grobler et al., 2010a). A strategy communicated from this level will ensure top management commitment and will promote the DFR framework downwards. It also ensures that resources and finances are allocated to facilitate DFR.

The illustration of the reporting line of the forensic unit ensures that stakeholders are aware which unit is responsible for handling forensic incidents (Grobler et al., 2010a; Grobler et al., 2010b).

It is also important for an organisation to identify their evidence-collection need; however, the use of the phrase *evidence collection methodology* rather than *evidence-collection need* is proposed for this study. The reason for this is that this sub-domain activity should also consider things such as evidence-gathering requirements. The use of the phrase *evidence collection methodology* is more encompassing and thus more suitable.

The implementation of this particular domain can assist with the realisation of a DF strategy and an evidence-collection statement to enable the alignment of business risk units with incident-monitoring units (Whyte & Claims, 2012). The finalisation of sub-domain activities in this domain can produce the following outputs:

- Organisation structure depicting the forensic unit and responsibilities
- DFR strategy that illustrates the objectives and goals
- Evidence-collection methodology.

Although this domain does not satisfy any of the goals and objectives as stipulated in Table1, it is an important part of DFR as it will ensure that DFR is driven from the senior management level down to ordinary staff. One could argue that a further purpose of this domain is to promote an enterprise-wide adoption of proactive digital forensics in an organisation.

Governance

This is a new domain within DFRCF and it advocates (a) the establishment of a DF policy frameworks and guidelines to ensure uniformity across the enterprise and (b) that governing bodies[5] should ensure that the policies and policy frameworks are implemented according to agreed standards (Grobler et al., 2010a).

Also, there must be a framework to calculate the costs of an incident investigation. Calculating the cost before an investigation will provide an indication of how successful, or not, their governance controls are (Grobler et al., 2010a).

The following are outputs that can be produced when completing the sub-domain activities within this domain:

- An evidence management (control) plan,
- An assessment of governance controls, and
- A framework to estimate costs of incidents.

This domain satisfies the following goals and objectives of DFR— as illustrated by Table12 below:

Table 12

DFR Goals and Objectives met by the Governance Domain

No	Objectives and Goals of Digital Forensics	Reference
6	To enhance the performance of IT & Info sec with DF tools in an organisation.	Grobler et al., 2010a; Grobler et al., 2010b
7	To demonstrate good governance by assessing the effectiveness of controls.	Grobler et al., 2010a; Grobler et al., 2010b

Systems and Events:

This domain ensures the identification and classification of hardware, software, processes, and events that house potential digital evidence. This is essentially a risk assessment that is conducted at business level (Rowlingson, 2004). The above activities will lead to systems and

[5] The governing bodies of an organisation are usually operational managers, strategic managers, and executive managers

infrastructure requirements as the organisation identifies the gaps that must be bridged to achieve its DFR objectives. New or improved technologies, hardware, software, and infrastructure might need to be acquired.

The establishment of a laboratory equipped with technologies and DF tools to do proper investigations is crucial within the DF realm (Grobler et al., 2010). The laboratory must strive towards ISO17025 certification as this validates that a laboratory is proficient to construct technically valid data and results (Wilsdon & Slay, 2005).

The following are all the possible outputs that can be produced when completing all the sub-domain activities within this domain:

- The identification and classification of source systems
- The identification of business events,
- Risk assessment,
- A list of systems and infrastructure requirements,
- A plan to acquire laboratory competence and accreditation.

This domain satisfies the following goals and objectives of DFR—as illustrated by Table13 below:

Table 13

DFR Goals and Objectives met by the Systems and Events Domain

No	Objectives and goals of digital forensic	Reference
1	To maximise an environment’s ability to harvest credible evidence.	Tan, 2001; Grobler et al., 2010b
2	To maximise the potential to use comprehensive digital evidence.	Grobler et al., 2010a; Grobler et al., 2010b
3	To minimise the cost of forensics during an incident response.	Tan, 2001
4	To gather evidence targeting the potential crimes and disputes that may adversely affect an organisation.	Rowlingson, 2004
8	To create proper data for good investigation leads.	Bradford et al., 2004

Policy

As noted earlier, there is a need to separate the Policy domain from the Compliance domain. This domain ensures that underlying policies and procedures are implemented according to agreed standards, as identified within the Governance domain. The following are examples of DF policies that can be implemented within an organisation (Barske et al., 2011):

- Policies about the acceptable use of information systems within the organisation.
- Policies that illuminate that source systems and their data within are the sole property of an organisation. A user must provide assurance that any data engaged with within the organisation will be monitored.
- Policies that inform the user how the source system will be monitored.
- Policies that inform when potential digital evidence will be preserved as well as what records will be preserved.
- Policies that indicate how long different types of digital evidence will be preserved and how they will be preserved and securely handled.
- Policies that indicate the conditions that will initiate an internal investigation and what actions might be taken in such an event.
- Policies that clarify the conditions under which digital evidence might be released to third parties such as law enforcement.
- Policies that clearly illustrate the responsibility, accountability. and roles that are involved in managing potential digital evidence and performing digital forensic investigations.
- Policies that clarify the legal review process in an event of a digital forensic incident investigation.

The above policies are possible outputs that can be produced when completing all the sub-domain activities within this domain. However, an organisation has to asses which policies are applicable and relevant to its entity. This domain satisfies the following goals and objectives of DFR— as illustrated in Table14, below:

Table 14

DFR Goals and Objectives met by the Policy Domain

No	Objectives and goals of digital forensic	Reference
5	To prevent anti-forensic activities.	Grobler et al., 2010a; Grobler et al., 2010b
9	To gather admissible evidence legally and without interfering with business processes.	Pangalos et al., 2010

Compliance

This domain was previously part of the Policy domain but has been separated because it is concerned with user conformance to legislation and DFR policies. A possible output that can be produced when completing all the activities within this domain is development of audit reports that measure conformance to governance requirements

This domain satisfies the following goals and objectives of DFR— as illustrated by Table15 below:

Table 15

DFR Goals and Objectives met by the Compliance Domain

No	Objectives and goals of digital forensics	Reference
6	To enhance the performance of IT & Info sec with DF tools in an organisation.	Grobler et al., 2010a; Grobler et al., 2010b
7	To demonstrate good governance by assessing the effectiveness of controls.	Grobler et al., 2010a; Grobler et al., 2010b

Training

This domain ensures that a DF training strategy is developed, DFR awareness campaigns are created, and that a DF training programme is developed. The training needs of the whole organisation must be assessed and accreditation must be sought for key forensic staff (Grobler et al., 2010a; Grobler et al., 2010b).

It is probably sufficient for the front desk operator to be aware of the forensic strategy and policies, but accreditation is crucial for the first responders as they will directly engage with the potential evidence, and the organisation would run the risk of evidence contamination if unskilled staff engages with evidence.

Laboratory certification must also be part of the training objective (Wilsdon & Slay, 2005). The ten-step process advocates role-play (DF incident simulation) training to ensure that all parties concerned are aware of decision-making points and actions (Rowlingson, 2004). It is possible to run DF incident simulations in conjunction with disaster recovery exercises.

The following are possible outputs that can be produced when completing the sub-domain activities within this domain:

- Awareness campaigns
- A training strategy with accredited training programmes.

This domain satisfies the following goals and objectives of DFR—as illustrated by Table16, below:

Table 16

DFR Goals and Objectives met by the Training Domain

No	Objectives and goals of digital forensic	Reference
11	To minimise interruption to the business from any investigation.	Pangalos, Ilioudis, & Pagkalos, 2010

Monitor and Report

This domain will ensure that organisations compile DF Incident report which comply with requirements (such as the report format, and so forth) and have an incident escalation policy. A cost analysis must be done before an investigation is commenced—to determine the feasibility of such an investigation (Rowlingson, 2004). The following are possible outputs that can be produced when completing all the activities within this domain:

- Reporting criteria (report format, report requirements, and so forth)
- Incident escalation policy
- Cost analysis
- A needs analysis for monitoring tools
- How IDS triggers should function and respond
- Guidelines (standards) for interaction between concerned parties (Whyte & Claims, 2012).

This domain satisfies the following goals and objectives of DFR—as illustrated in Table17 below:

Table 17

DFR Goals and Objectives met by the Monitor and Report Domain

No	Objectives and goals of digital forensic	Reference
5	To prevent cybercrime activities.	Grobler et al., 2010a; Grobler et al., 2010b
9	To gather admissible evidence legally and without interfering with business processes.	Pangalos et al., 2010
10	To allow an investigation to proceed at a cost in proportion to the incident.	Pangalos et al., 2010
11	To minimise interruption to the business from any investigation.	Pangalos et al, 2010

Legal Requirements

This domain was named the Legal involvement domain; however, this name will be changed to the Legal requirements domain as it provides a better description of the accompanying activities. This domain ensures that judicial, regulatory, and other laws within the organisation's realm of operation are considered and incorporated in the overall DFR strategy. It must inform all outcomes within the framework (Rowlingson, 2004; Whyte &

Claims, 2012). The following are possible outputs that can be produced when completing all the activities within this domain:

- Legal requirements
- Judicial requirements
- Other lawful requirements
- Business requirements.

This domain satisfies the following goals and objectives of DFR—as illustrated by Table18, below:

Table 18

DFR Goals and Objectives met by the Legal Requirements Domain

No	Objectives and goals of digital forensic	Reference
4	To gather evidence targeting the potential crimes and disputes that may adversely impact an organisation.	Rowlingson, 2004
9	To gather admissible evidence legally and without interfering with business processes.	Pangalos Ilioudis, & Pagkalos, 2010
12	To ensure that evidence makes a positive impact on the outcome of any legal action.	Pangalos, Ilioudis, & Pagkalos, 2010

The extended DFRC framework-v1 incorporates the best of the DFRC and the DFM frameworks. This study married all the goals and objectives, as identified in Table1 of this study, to the extended DFRCF model. It is thus reasonable to declare that the DFRCF model, when managed to perform all the activities within the domains, will ensure that all the goals and objectives of DFR are met.

Furthermore, the DFRCF provides an opportunity to contribute to the enhancement of the goals and objectives of DFR. The activities within the Strategy domain could not be reconciled to the existing goals and objectives and therefore this study includes the following goal in the list of goals and objectives: *To promote an enterprise-wide adoption of proactive digital forensics.*

The possible reasons why existing frameworks do not reconcile (align) with the goals and objectives of DFR could be because (a) no previous attempts had been made to reconcile the goals and objectives with the frameworks, and (b) it is possible that researchers do not understand the benefits of such an alignment.

There are several frameworks, or at least interventions, that seek to align the one or other entity (or activity) with another entity (or activity). The overall alignment model is an example of a model that seeks to align information technology with business strategy (Henderson & Venkatraman, 1993). A similar model was presented by Luftman et al, and called the strategic alignment model (Luftman, Lewis, & Oldach, 1993). It is reasonable to conclude that the misalignment of entities that should be aligned has undesired effects on a business, hence, the resources used and the efforts made by organisations to align these activities, post implementation. It would therefore be preferable to develop a DFR framework that is aligned with the objectives and goals of DFR—such as the DFRCF.

It is necessary for this study to verify/validate the DFRCF-v1 so that its significance and relevance can be attested in the DFR domain (Soni & Kodali, 2013, p. 275). A verified framework promotes frequent use and frequent use promotes generalisation (Soni & Kodali, 2013, p. 275).

Chapter Summary

The extended DFRC framework harnesses the best of the DFRC and the DFM frameworks. The domains and sub-domains of the extended DFRCF form the structure of DFR and help to answer the first part of the research question that seeks to understand "*What DFR structure (elements or domains) is needed by financial services businesses*".

The extended framework not only illustrates which goals and objectives of DFR are realised, but it also contributes to the body of knowledge by adding a new objective, namely: to promote an enterprise-wide adoption of proactive digital forensics.

In the following chapter, the research design and methodology that was utilised in this study will be discussed.

CHAPTER 4: RESEARCH DESIGN/METHODOLOGY

In this chapter, the framework that was utilised to select the research methodology, the data collection technique, and the subsequent data analysis is discussed. The chapter briefly presents the definition of research, investigates quantitative and qualitative methodologies and mixed methods, and describes the reason the selected methodology was chosen over another. Lastly, the tool and data analysis techniques are described.

Research

Research as an activity that collects large quantities of information, explores cryptic theories, and constructs new products (Walliman, 2006). Research is also conducted to increase knowledge (Amaratunga, Baldry, Sarshar & Newton, 2002). This broadens the field of knowledge in each discipline in which it is conducted.

Research Philosophies

It is important to illustrate the rationale behind the selection of research philosophies and approaches (Dilley, 2004). First is the consideration that the study will be examined by dissertation committee members and institutional review boards who might follow diverse approaches and who must be convinced that the approach employed is suitable.

Second, the selected framework should help the researcher understand what the strengths and weaknesses of the particular approach are (Dilley, 2004). Third, the researcher has to comply with the guidelines provided by the approach; deviations could be unscientific and could nullify the research. Lastly, the approach also prescribes the researcher’s role, whether he/she should reveal personal opinions or remain neutral (Dilley, 2004).

The above statements advocate compliance and non-deviation to the research frameworks; however, the field of Information Systems (IS) had been employing philosophies and approaches from other subject areas whilst not necessarily understanding the underlying assumptions (Dobson, 2002). This study will provide a summary of epistemology and ontology to illustrate the understanding of the two philosophies.

- Epistemology is interested in how knowledge is acquired and what can be regarded as adequate knowledge (Walliman, 2006). It focuses on the association between the entity being observed and the observer (Corbetta, 2003).
- Ontology is concerned with understanding of whether entities exist in their own right or of they only exist within the human mind (Corbetta, 2003).

The figure below depicts the research pyramid as introduced by Jonker and Pennink (Jonker & Pennink, 2009). See Figure 8.

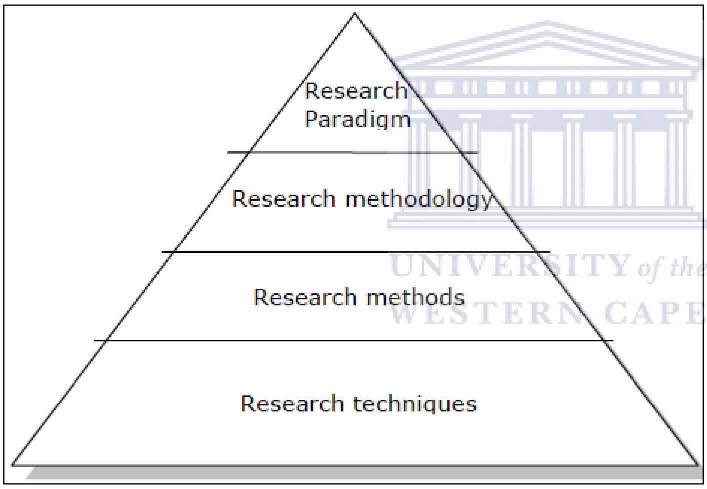


***Figure 8*: Research pyramid (Source: Jonker & Pennink, 2009, p. 23)**

The pyramid portrays a graphical illustration of the research journey. It has four research levels—paradigms, methodology, methods, and techniques—that are a series of interrelated events and decisions, ranging from the abstract (paradigm) to more technical (techniques) events. The model, as proposed by Jonker and Pennink (2009), aims to inform the reader of the decisions that need to be taken as he/she progresses through the research journey and it also reveals the available alternatives to techniques and tools.

This study will elaborate on the four levels and demonstrate their applicability to this study. Literature from other sources will also be incorporated to strengthen the argument for the chosen research methods, but emphasis will be placed on information that is relevant to this study.

Research Paradigm

The term "research paradigm" is related to how the person performing the research observes reality (Gummesson, 1999). This is also referred to as *the researcher's basic approach*. It comprises the underpinning rules and values that motivate the thinking and behaviour of the researcher (Gummesson, 1999). There are several types of paradigms or perspectives, as noted below:

- Knowing through the eyes of someone else—means that the full facts only become known through proper examination of a phenomenon. An example of this is research that is conducted to measure how employees feel towards their employer.
- Knowing through the eyes of the researcher—is where a researcher can create an idea of the reality through available literature and then later has the idea validated. An example of such research is this study. The researcher has an idea of the reality (state of DFR maturity models) and most of the information is available through literature, but the end result (model) will be tested with practitioners. This means that this study is made known by looking at research through the viewpoint of the researcher. There is no choice to be made in this particular paradigm. The nature of the research determines the paradigm.
- The other approaches proposed are (a) positivism—conducting researching without considering implementation requirements, (b) constructivism—research conducted from within the confines of the subject and learning and growing with the subject, (c) empiricism—similar to positivism, but data and facts are emphasised without any

reliance on theory, and (d) interpretivism—research that suggests that events can be better understood if the people performing the action is placed in the social context (Kelliher, 2005).

Research Methodology

There are several definitions contextualised to define what is meant by research methodology. Mackenzie & Knipe, S. (2006), pp 193-205, summarise some of the definitions as (a) "the collection of methods or rules by which a particular piece of research is undertaken", (b) "principles, theories and values that underpin a particular approach to research", and (c) "the frame of reference for the research which is influenced by the 'paradigm in which our theoretical perspective is placed or developed' ". All of the above definitions are contextually correct and it can therefore be argued that a methodology highlights the direction to a destination, but that does not detail the associated steps. There are primarily two types of methodologies or approaches: qualitative and quantitative. However, the two approaches can be combined in a single research to examine different levels of the same phenomena. This combined methodology is called *mixed methods* (Johnson, Onwuegbuzie & Turner, 2007).

Qualitative methodology

Qualitative methodology is aimed to provide rich, in depth, and illustrative accounts of the investigated entity (Geertzt, 1973). It is specifically aimed at behavioural science to discover underlying intentions and motives (Goddard & Melville, 2004).

In this study, the qualitative methodology has been adopted to understand the first part of the research question, namely: "*What DFR structure (elements or domains) is needed by financial services businesses?"* Table 2, in Chapter 2 of this study, lists the different frameworks and also highlights the approaches taken by each study. The approach and the framework employed in this study to answer the first parts of the research question are consistent with approaches and frameworks taken by researchers cited from the reviewed literature. This study has therefore adopted the widely accepted approach based on Table 2.

A qualitative methodology is used in this study to answer the second part of the research question, namely, “*How can such a structure contribute to the design of a maturity assessment model?”* The second part of the research question considers (a) the design process of a maturity assessment model and (b) the construction of the maturity matrix and it provides their definitions. Authors of relevant literature have suggested the use of interviews, Delphi studies, case studies, and focus groups to derive the characteristics of a maturity model (Pöppelbuß et al., 2011). This indicates a qualitative approach (Raber, Winter, & Wortmann, 2011). Furthermore, the use of words, open questions, and discussions are a more appropriate approach to gather the data required to populate the assessment model. Researchers of associated literature have discouraged the use of quantitative methods for designing maturity models because the researcher would have to employ valid data sets and have familiarity with statistical methods; hence, they are less often used for designing maturity models (Fraser, Moultrie, & Gregory, 2002). Lastly, the design process that this study followed is based on the design process recommended by authors of the literature consulted on this topic. Thus, the approach and framework taken in this study to answer the second part of the research question is consistent with approaches taken by similar research studies.

Quantitative methodology

This type of research is aimed at putting together events and volumes and looking at relationships between entities. It reduces the investigated entity to numerical values to perform statistical analysis (Gelo, Braakmann, & Benetka, 2008).

It is regarded as research that is based on facts reflected through exact figures (Jonker & Pennink, 2009). It is a strictly goal-oriented procedure which aims for objectivity (Flick, 2011) and is based on the measurement of amount or quantity.

Mixed methods approach

This is the integration of qualitative and quantitative methodologies to garner a better understanding than is possible with either methodology alone (Creswell, 2003, p. 5). There are two major types of mixed methods (Johnson and Onwuegbuzie, 2004, p. 20):

- Concurrent or simultaneous—this is where dissimilar research methods are integrated into one research to enable a singular interpretation of the results.
- Sequential—this is where the research starts off with one method but is followed by another method or several other methods.

According to Johnson and Onwuegbuzie (2004), the following are rationales for conducting mixed methods research:

- Triangulation—is the verification of results by employing different methods.
- Complementarity—the findings of one method are clarified or enhanced by employing the results of another method.
- Initiation—the achievement of new insights that will encourage new research questions.
- Development—a method is shaped by the results of another method.
- Expansion—the focus is to expand the scope and penetration of research by using dissimilar methods to investigate different angles of enquiry.

Research Methods

A method highlights specific phases or actions to be taken in a specific order during the research journey. It is the systematic approach to collect and analyse data to glean meaningful insights from the data presented (Jankowicz, 2000, p. 209).

According to literature, the main research methods are experiment, survey, case study, grounded theory, ethnographic and observational methods, and lastly, action research (Gable, 1994; Kuo, Dunn, & Randhawa, 1999; Charmaz, 2007; Gelo et al., 2008).

Experiment

This is where the researcher makes conjectures about relationships between an unconnected anomaly and another (or more) connected anomaly(ies). It usually involves the manipulation of a variable or relationship (Gelo et al., 2008). This research is not involved in experiments or manipulation of relationships and as such this research method would be inappropriate for this study.

Survey

This is refers to a cluster of quantitative analysis methods where large quantities of data are collected using methods like questionnaires and interviews (Gable, 1994). This study requires in depth discussions and it must allow for new data to be discovered. Survey research is an inappropriate method for this study because surveys cannot be structured to provide depth and richness of the topic and this method does not allow the discovery of new data.

Case study

Case studies allow the researcher to collect in-depth information as they permit interviewees to describe experiences in their own manner and not in a manner prescribed by the researcher (Kuo, Dunn, & Randhawa, 1999). This study employed the case study method because it has been utilised by similar research (Pöppelbuß et al., 2011). Secondly, this approach is selected because all the other methods have been shown (see other research methods) to be inappropriate for this study.

Grounded theory

This approach allows the collection and analysis of data to happen simultaneously. This iterative approach between empirical data and results of analysis makes the data collection more refined (Charmaz, 2007). This is an iterative approach that seeks to ground and refine the theory as new data becomes evident. This study will not have multiple iterations and therefore cannot be classified as grounded theory.

Ethnographic and observational methods

These are means of collecting data in which the researcher seeks to become part of a group and by being part of the group or the event, hopes to collect more data than would had been possible if the researcher was not part of the event or group (Vinten, 1994). This method is largly used to study groups of individuals or events as they happen. This study will not perform any of the mentioned actions and will therefore not utilise this method.

Action research

It is a free process that focuses on creating practical know-how in the search of meaningful social purposes (Reason & Bradbury, 2001). Action research can also be considered as the research that is concerned with the investigation alongside people rather than the investigation about people (Altrichter, Kemmis, McTaggart, Zuber-Skerritt, 2002). This study will not utilise action research because the study does not focus on people but it focuses on a process.

Research Techniques

This is an exact step-by-step procedure that can be taken to gather and analyse data for further exploration (Jankowicz, 2000, p. 211). There are (a) structured techniques—usually a series of questions with pre-set possible answers, and (b) semi-structured techniques—usually a defined theme that allows for open responses. Techniques are use synonymously with tools or instruments (Jonker & Pennink, 2009, p. 25).

Structured technique

The following are the various types of structured techniques:

- Questionnaires—used for collecting large data with closed questions. They are usually used with a Likert-type scale.
- Repertory grid—is similar to the questionnaire, but the researcher involves the subject in designing the questions.
- Structured interview—different participants will be interviewed and confronted with the same question sets.
- Structured observation—is mostly performed by machines such as electronic point-of-sale applications that observe a user's selection of products.

Unstructured technique

The following are the types of unstructured techniques:

- Unstructured observation—implies the use of the respondent's notes, diaries, and so forth.
- Focus group—this is when a number of people are assembled to discuss a particular subject and the discussion is recorded.
- Conversation—this tool is utilised when an informal conversation touches on the research topic.
- Semi-structured interviews—are used when there is a particular theme and leading questions for the interview, but the interviewee allows for slight deviation in the theme to better understand the subject as a whole. This style opens itself for possible new discoveries which are otherwise not available with structured interviews.

This study employed interviews to collect data from practitioners who are concerned with DFR. The interviews were both structured and semi-structured in nature. Literature concerned with developing assessment models suggested the use of interviews, Delphi studies, case studies, and focus groups to derive the characteristics of a maturity model (Pöppelbuß et al., 2011). This study selected this technique because the alternatives, such as

Delphi studies and focus groups required a convergence of participants in a central place, for multiple iterations. This was impossible to achieve without a sizeable budget (administration, venue, tools, refreshments, and so forth) and disruption to the lives of the participants, since some of them were located in other provinces. A case study technique would have been ideal, however most of the participants could not provide proprietary artefacts and one participating organisation did not have a formal forensic process. Thus this technique was the most feasible for this study. The interviews were both structured (to give direction) and semi-structured (to allow for the discovery of new information). The interviews were conducted with willing and available participants. The conversations were recorded during the interview and then transcribed post interview to enable the researcher to replay the conversations and to allow other researchers to access the same data.

Instrument Design—Interview:

Digital Forensic (DF) Practitioners within the Western Cape of South Africa were consulted and asked leading questions regarding domains and sub-domains within DFR, maturity levels, and their descriptions and measurement criteria (see Appendices 1 and 2 for the proposed question set and the models that initiate the discussions). The set of questions in Appendix 1 seeks to elicit responses that will enhance the proposed DFR framework. The questions in appendix 2 are designed so that participants select either a check-box (tick box) assessment approach or a quantitative assessment approach. The participants in the study used the check-box and the tick-box concepts interchangeably.

Sample Design:

Sample design is described as a plan to gather a sample from a population (Goddard & Melville, 2004). They further classify sampling as either *probability* sampling (there is an equal probability of inclusion in the sample) or *non-probability* sampling (probability of inclusion cannot be determined).

Examples of probability sampling are area sampling, systematic sampling, stratified sampling, and random sampling. On the other hand, quota sampling, judgement sampling, and convenience sampling are associated with non-probability sampling.

The topic of forensic readiness is sensitive and few organisations are willing to have their forensic information publicised (Whyte & Claims, 2004). With this in mind, random sampling from a list of South African long-term and short-term insurance companies and of South African banks and private forensic companies was adopted for this study. The list of long- and short-term insurers was downloaded from the financial services board website (www.fsb.co.za) under the *list registered insurers* section and the list of banks was retrieved from the South African Reserve bank website (www.resbank.co.za) under the *regulation and supervision* section. The lists of private forensic companies were companies that were known to the researcher.

The sampling process was markedly challenging since it was difficult to find the correct sample composition. The preferred sample composition consists of companies that

- provide a financial service
- have a digital forensic footprint
- are willing and able to contribute to the study, and
- are suitably knowledgeable about digital forensic readiness.

With this constraint foremost in mind, the study interviewed a minimum of 10 participants. Two of the interviewed participants are well-known, respected, and influential in the computer forensics circles in South Africa; and one of them has had several digital forensics articles published. The rest of the interviewees are all in leading positions within their respective organisations. The sample is therefore composed of well-connected and experienced participants.

Data Analysis:

Data analysis is the process of reducing the data to a more manageable size so that common themes and patterns can be exploited (Cooper & Schindler, 2001, p. 82). This view is echoed by Goddard and Melville (2004), who suggested that data should be classified into purposeful and usable categories.

Qualitative data analysis is not an easy, off-the-shelf, one-fits-all approach (Creswell, 2007; Miles & Huberman, 1984). With this said, however, authors of research literature suggest that researchers (a) must organise the data, (b) become acquainted with the data, (c) classify or code the data, (4) interpret the data, (5) and present the data.

Organising data: The audio recorded interviews were each transcribed into separate Word documents. A half an hour's recording roughly translates to12 pages of transcription.

Become acquainted with the data: The transcriptions were studied and edited for correctness.

Classify the data: The data was classified into themes based on the DFR domains and each participant's response was recorded against the particular domain.

Interpret the data: The participant responses were analysed for consistency and conflicting views. The aim in this study was also to understand the relationships between respondent expertise, industry, feelings, and views.

Data presentation: The key findings of this study will be presented in chapter 4.

Unit of analysis

The domains and sub-domains were the units of analysis. All questions and responses were organised under the domains and sub-domains.

Interviews

In all, 10 interviews were held with 10 participants. Two interviews were performed through Skype because of the distance between interviewer and interviewee. Interviews lasted from 7 to 36 minutes and were audio-recorded with the consent of the participants.

Data management

The management of data is important for qualitative research because it ensures validity, reliability, and transparency, and it ensures that the information is kept in a manner that allows other researchers to draw similar conclusions.

The interviews were recorded electronically using an electronic voice recorder. The recordings were transferred to a laptop and stored under separate folders. Each folder housed the recordings and artefacts that were collected during the interview. Each folder was named to reflect the name of the participant(s), for example, an interview with consultant John Doe was named "DFR interview with John Doe". The audio recordings were transcribed using Microsoft Office Word 2007 and the transcriptions were renamed consistently, according to archiving rules (Mack, Woodsong, Macquee, Guest, & Namey, 2005).

The transcript name contained the site name, data-gathering method, practitioner category and a sequential number. For example, if the third interview was held with DF consultant John Doe at Pick 'n Pay offices, then the transcript name would be PPFICO03, the site name would be (PP) Pick 'n Pay offices, the data-gathering method would be (FI) formal interview, the practitioner category would be (CO) consultant, and the sequential number would be (03) third data collection interview.

The transcription template (see appendix 3 to see an example) used in this study is an adaptation of a template based on the article *Qualitative Research Methods: A Data Collector's Field Guide* (Mack et al., 2005, p.109).

The Minnesota Oral History Association suggests several transcription conventions (Minnesota Historical Society, 1996). The following transcription conventions were adopted in this study:

- Ellipsis points (…) which imply hesitation, changing a thought or uncertainty. Example: "I bought … how much did that cost?"
- Square bracket ([ ]) is used to provide information that is not visible to the reader or to indicate that the narrator used a word that the narrator thinks was used. Example: "When the study [Unclear] subject three".
- EM dash (—) signifies that the speaker trailed off, did not finish the words or was permanently interrupted. For example,

  "John: Can you—

Mary: Where were you?

John: I was at home, working on my assignment."

Data confidentiality

Computer forensics is a sensitive subject for many organisations especially in a competitive market where forensic readiness can be considered a competitive advantage. Therefore, in this study, the identities of participants are withheld and a standard naming convention applied. All respondents are referred to as *participants* and a number is allocated them in the sequence of the interview. In other words, participant one was interviewed first and participant seven was interviewed seventh. The organisations in which the participants are employed are not named, but the industry in which the organisation operates is instead referred to.

Summary of Chapter

Data pertinent to the DFR structure and maturity assessment model was collected and presented. The DFR structure is encapsulated by the domains and sub-domains and as such feed back to the research question. The domains also feed into the maturity assessment model.

Data was collected through semi-structured interviews. The two open ended questions prompted discussions on the DFR domains and maturity assessment model. Random sampling was employed due to a lack of willing participants and expertise. The data was analysed and classified according to the DFR domain themes. The subsequent data will be utilised to design the maturity assessment model.

In the following chapter (findings and presentation of results), the key findings of the data collection will be highlighted and discussed.

CHAPTER 5: FINDINGS AND PRESENTATION OF RESULTS

This chapter presents the findings of data collected through interviews. The chapter is divided into three main sections. The first section addresses data confidentiality, sample selection, and the demographics of the participants. The middle section (Results) deals with the findings around the eight digital forensic readiness domains and their sub-domains. The domains and sub-domains represent the DFR structure and as such are associated to the research question. Each domain is discussed separately to keep the dialogue uncluttered.

The last section focuses on practitioner responses to the two proposed maturity assessment models.

Participant Demographic

Tables 19 and 20 below illustrate the participant profile/demographics.

Table 19

Participant Demographics

Participant	Years of forensic experience	Industry where most forensic experience gained.	Contributed forensically to more than one industry? Please state all	Size of current company
P1	5	Long-term insurance	No	> 10 000
P2	8	Long-term insurance	No	15,000 staff in SA and 40, 000 staff internationally
P3	14	Not available	Yes	1001 - 5000
P4	20	Short-term insurance	Not available	> 2300
P5	7	Not available	Not available	501 - 1000
P6	11	Banking		1001 - 5000
P7	16	Law enforcement	Yes, across several industries	655
P8	14	Public Sector, Mining	Mining, Oil, Public Sector, Technology, Gaming	N/A. Have retired
P9	Participant information not available			
P10	14	Long-term insurance	No	About 3000

Table 20

Participant Demographics (continued).

Participant	Highest forensic education	Board member of any organisation in a forensic capacity	Have implemented forensic measures that are widely adopted by an organisation	Have recommended forensic measures that are utilised across industries
P1	BCom Honours (Computer Forensics)	No	No	No
P2	BCom Honours (Computer Forensics)	No	Yes	No
P3	Mtech	Yes	Not available	Not available
P4	Not available	Yes	Not available	Not available
P5	BEng	Not available	Not available	Not available
P6	MBA	Not available	Not available	Not available
P7	Master's degree	Association of Certified Fraud Examiners	Yes	Yes
P8	CISSP	No	Built the forensic framework for a large financial services organisation and done training for many organisations across the globe	No
P9	Participant information not available			
P10	Diploma in Criminal Justice & Forensic Auditing	No	Yes, one organisation	No

The above table displays the demographics of the participants. The table shows the industries in which they operate, their forensic experience, the size of the company, their highest forensic qualification, and so forth. The opinions of highly qualified, multi-industry, experienced participants who have had their forensic work published and are board members in a forensic capacity are valuable.

Results

The objective of this section is to present the key responses to questions posed to answer the research question. The participants were presented with domains of the DFRCF and asked how the model might be refined. Responses to the open-ended question (*Find the above domains: how would you improve on them and can the sub-domains be further refined?*) stimulated more discussions between the interviewer and subjects. The resultant discussions encouraged the practitioners to improve the model by moving the domains and sub-domains around, renaming or discarding them. The expected outcome was a well-thought through, vetted DFRCF and DFR maturity assessment model that satisfied the need of this study.

For ease of reading, the study highlighted the changes proposed by the participants. Borders with dashed lines were drawn around elements that (a) were moved from one domain to another, (b) experienced name changes, and (c) introduced as new elements for the first time. See Figure 9 below as an example.

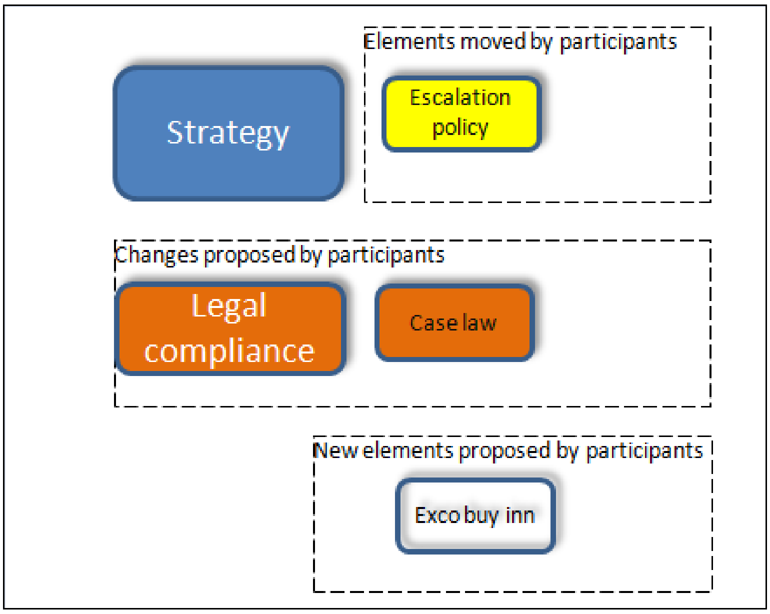

Strategy
Elements moved by participants
Escalation policy
Changes proposed by participants
Legal compliance
Case law
New elements proposed by participants
Exco buy inn

***Figure 9*: Legend illustrating the types of changes proposed by participants.**

DFR Domains and Sub-Domains (DFR Structure)

Strategy domain

Six of the participants agreed completely with the elements presented and did not propose any changes. These participants originate from the following industries: long term insurance, short-term insurance, investment services, banking, and risk consultancy. Figure 10 illustrates the proposed elements.

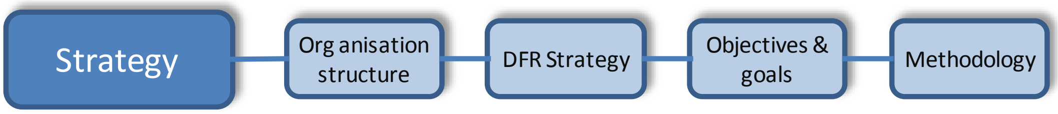


***Figure 10*: Proposed Strategy domain with its sub-domains.**

The public sector was the only industry that proposed changes to the Strategy domain. The proposed changes were minor as the participant suggested that the DFR strategy and methodology should be combined and renamed *Strategic framework*.

Participant 8 agreed with the original proposal but suggested that business requirements move from the Legal requirements domain to the Strategy domain. On the other end of the spectrum were participants 1 and 2, who dismissed the entire domain. The reason for this omission remains unexplained, but the size of their multinational long-term insurance organisation might provide a hint to their complex operating environment, which probably requires a different structure to those of smaller organisations.

Legal requirements domain

Figure 11 below illustrates the original proposed domain and sub-domains.

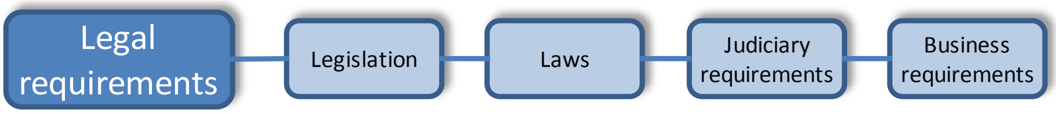


***Figure 11*: Proposed elements of the Legal requirements domain.**

This domain encouraged a good deal of discussion and there were various views on what the domain should look like. The following are some of the changes encouraged by the participants.

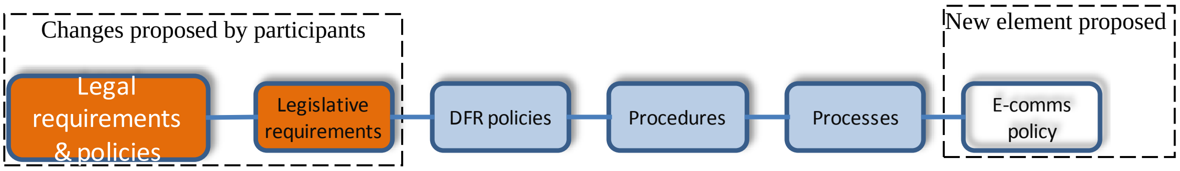


***Figure 12*: View expressed by participant number 4.**

Participant 4 had the most disparate view, as shown by Figure 12 and compared against the original model (Figure 11). The participant who is employed in the short-term insurance industry suggested that the Policy and the Legal requirements domain be merged, saying, "*Most of your policies are derived from legislation. You definitely got this link between policy and legislation. There must be a link. So can I do that for you?*" and "*So policy and legal requirements generally go hand-in-hand*".

Following his recommendation, the domain was renamed Legal requirements and policies and the legal sub-domains (legislation, laws, and judicial requirements) were also combined and renamed Legislative requirements. Furthermore, the participant also included the Electronic communications policy as part of the domain—hence the clear-coloured element.

Participant 7 (employed in the public sector) revealed a thorough understanding of the intention of the domain and the subjects within the domain. Figure 13 reflects his position.

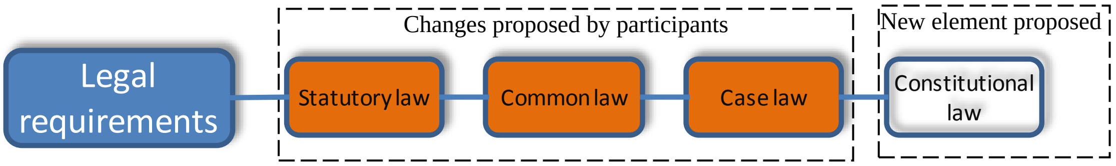


***Figure 13*: Participant 7's view on Legal requirements**

The participant renamed all the following sub-domains: Legislation became *Statutory law*, Laws became *Common law*, and Judicial requirements became *Case law*.

Similarly, participant 8 also used the term *Case law* to describe the prevailing philosophy around court cases: "*I would have something separate that says case law or current thinking in terms of court*." The words *current thinking* were used to stress that courts have a manner of interpreting cases or evidence and that companies must take cognisance of such thinking (ideas) and ensure that their evidence meets these ideological parameters. Participant 8 continued on this track by including a new sub-domain: *Judicial readiness*.

Participant 7 also introduced a new sub-domain: Constitutional law. The idea is that all laws are subject to it and as such must be factored in policy designs. The exact words were *"I think, in any organisation, that doing some sort of legal issue around forensic readiness, the constitution has to be considered issue"*.

Both participants 7 and 8 removed Business requirements from the domain. The understanding is that the business requirements are ultimately a reflection of the legal requirements.

In summary, the elements that enjoyed the most consensuses are displayed in Table 21 below.

Table 21

Legislative Domain—Elements That Received the Highest Consensus

Element	Number of consensuses
Legislation	7
Judicial requirements	7
Laws	6
Business requirements	5

Governance domain

Participants 4 (short-term insurance) and 5 (investment company) agreed completely with the proposed Governance domain and made no changes (see Figure 14 for the proposed domain model).

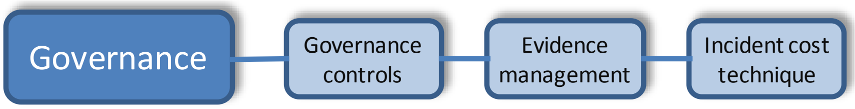


***Figure 14*: Governance domain of the DFRCF.**

Participants 9 and 10 suggested only minor changes which entailed the removal of the Incident cost technique sub-domain. Their particular forensic unit within the organisation (a large insurer) is mandated to investigate each and every incident that is directed to them. Their business requirements dictate that all incidences are investigated and they argue that this element is solely appropriate in an event where the investigation is outsourced.

Respondent 10 observed, "*So it is not as if we are going to outsource our services and we need to attach a cost structure*." This view was echoed by a colleague, respondent 10, who said, "*We are not going to be a consultant [contact] or something*".

Thus, it is pertinent to note that all three participants (participants 3, 7, and 8), who are forensic consultants, proposed significant changes to the model (see their respective models in Figure 15, Figure 16, and Figure 17)

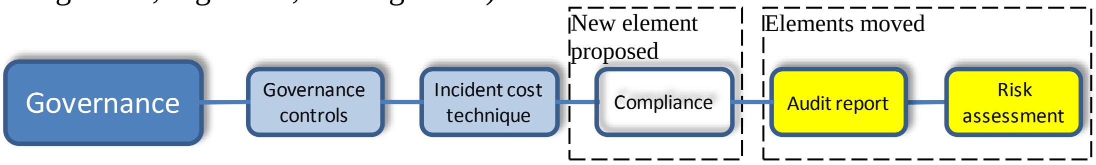


***Figure 15*: Governance domain according to participant 3.**

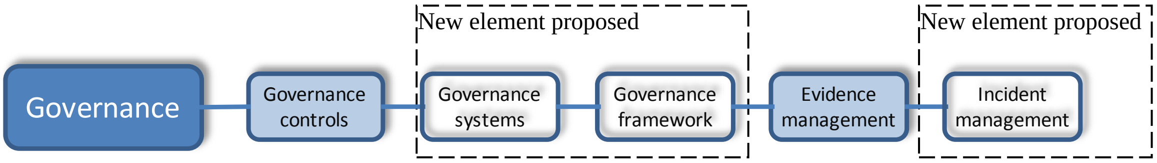


***Figure 16*: Governance domain according to participant 7.**

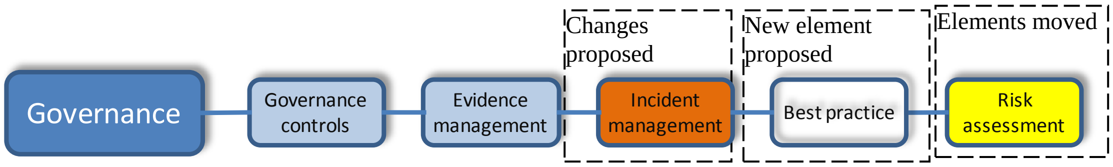


***Figure 17*: Governance domain according to participant 8.**

All three above participants agreed that governance controls should be part of the domain. Two agreed that evidence management should remain within the domain and both recognised the value of having an incident management sub-domain. The tallied argument was, "*Once you have identified that you have an incident, what needs to happen then*?" Hence, the addition of the incident management to illustrate that a process is available that describes *how, what,* and *when* incidences need to be managed.

The Risk assessment element was moved from the Systems and events domain to the Governance domain by participant 3 and 8. Participant 3 argued that the King III Report (code of global best practices for corporate governance in South Africa) places the activity of risk assessment under governance so this model should be added as a best practice standard: "*The King III Report, the governance thing? Risk assessment there will fall under governance*".

Other new elements that were introduced were: Governance systems, Governance framework (by participant 7), Best practice (by participant 8) and Compliance by participant 3. Participant 3 maintained that compliance is an integral part of governance but admitted that governance was not his area of expertise: "*I am not an expert on governance issues and those types of things*".

On the other hand, participant 7, who "*deal[s] with compliance on a regular basis*", did not incorporate it under governance, but kept the Compliance domain separate.

In summary, the elements that drew the highest consensus are displayed in Table 22 below.

Table 22

Governance Domain—Elements that Received the Highest Consensus

Element	Number of consensuses
Governance controls	8
Evidence Management	7
Incident cost technique	3
Risk assessment	3

Systems and events domain

Figure 18 below illustrates the proposed Systems and events domain model that was presented to the interviewees.

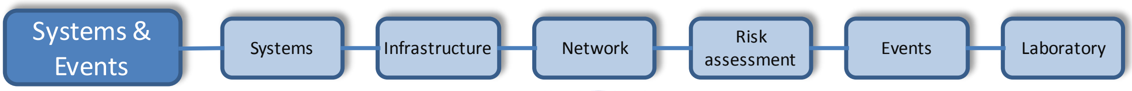


***Figure 18*: Proposed elements of the Systems and events domain.**

Participants 9 and 10 agreed completely with the proposed model and had no changes. Participants 4, 5, and 6 agreed with the complete model, but discarded the Risk assessment element from the domain. Participant 4 is a practitioner in the short-term insurance field and participant 5 is a practitioner in the investment industry. Although the participants hail from dissimilar industries, their thinking is aligned, as both of them created a new domain and moved the Risk assessment element to the new domain. This could signify that the DFR structure is fairly similar for these two industries and that the DFRCF model might apply to both. This is also evident in their responses to the reasons for moving the Risk assessment element out of the Governance domain (see Table 23).

Both participants are of the opinion that the business and risk environment has to be understood, and that mitigations should be put in place to deal with said risk exposure.

Table 23

Illustrates Similar Comments Made by Participants 4 & 5

Participant	Participant response	Line #	Transcript file
Participant 4	…you will analyze your environment; what the defects are, what need to be done to keep those defects…What are the typical risks or exposure…How will you mitigate those risks?	137, 138, 141-143, 158, 159	MFFIPR04
Participant 5	…it should cover the understanding of the business environment, it should understand the typical risk in that environment, how the risk should be mitigated … highlight control deficiencies, and then put actions in place	6-10	N/A

The only changes made to the domain name came from participants 1 and 2, who renamed the domain Technology. The reasons for the name change could not be confirmed with the participants; however, it is possible that it has to do with the fact that the Events element was removed from their model and thus needed to be renamed to avoid confusion (see Figure 19 below).

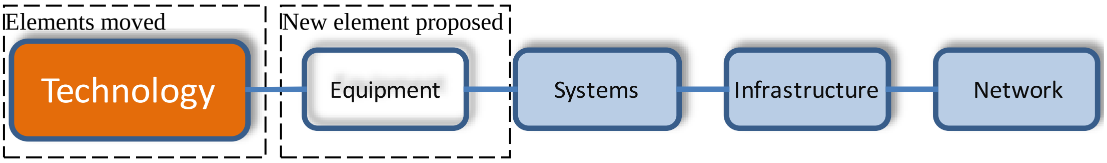


Figure 19: Systems and events—comments made by participants 1 and 2.

The most extensive comments were received from participant 7, who is the most senior and most recognised forensic authority included in this study. The participant has also published various research articles related to DFR, some of which have been cited in this study (see Figure 20 for an illustration of his interpretation).

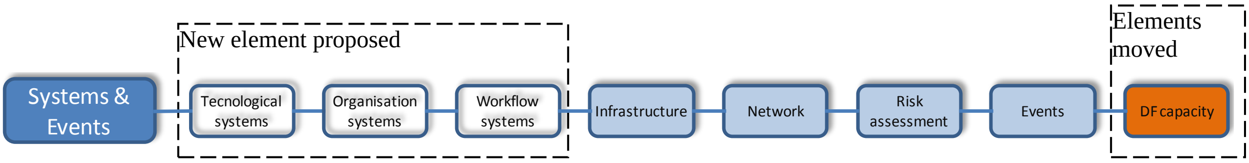


Figure 20: Systems and events—comments made by Participant 7.

The participant renamed Laboratory to DF capacity. He argued that laboratories are only found in large organisations and that *laboratory* refers to a physical structure, which is not always the case for smaller organisations. Hence, it should be renamed DF capacity as the domain actually seeks to ensure that there is some form of forensic ability and skill, rather than being a facility. The participant also proposed that the Systems element should be sub-divided into Technological systems, Organisation systems, and Workflow systems.

In summary, the elements that enjoyed the most consensuses in this domain are reflected in Table 24 below.

Table 24

Systems and Events Domain—Elements Receiving the Highest Consensus

Element	Consensuses total
Infrastructure	9
Network	9
Systems	7
Events	7
Laboratory	5

Policy Domain

Figure 21 illustrates the proposed Policy domain model that was presented to the interviewees.

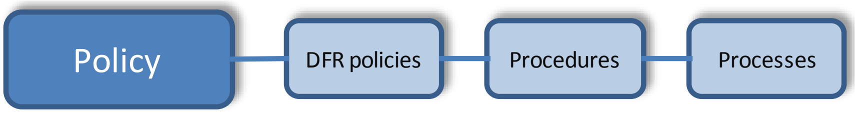


***Figure 21*: Proposed elements of the Policy domain.**

This study understands that consistency enhances the reading experience; however, due to the number of changes and additions to this domain, this study will change the presentation of the results to a tabular format to enable the display of multiple data.

Table 25 below is an illustrative view of participant responses to the proposed Policy domain. The table headers are explained as follows:

- *Element* refers to the sub-domain; the terms are used interchangeably in this study to enable better reading. For example, "the Risk assessment sub-domain was moved to the Governance domain" reads better as "the Risk assessment element was moved to the Governance domain".
- *Type* distinguishes between (1) *proposed*—the original elements that were proposed to the participants, (2) *moved*—elements that were shifted around between domains, (3) *changed*—elements that were modified by the participant, and (4) *new*—elements that are introduced to the model for the first time.
- P1-P10 are participant numbers from 1 to 10.

Table 25

Proposed Elements of the Policy Domain

Element	Type	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10
DFR policies	Proposed	√	√		√	√	√	√	√	√	√
Procedures	Proposed	√	√	√	√	√	√	√	√	√	√
Processes	Proposed	√	√	√	√	√	√	√	√	√	√
Escalation policy	Moved	√	√	√			√		√		
Evidence management	Moved			√							
Incident cost technique	Moved						√				
Business requirements	Moved									√	√
Legal policies	Changed			√							
Procedural policies	New										
Reporting processes	New			√							
E-comms policy	New				√	√					
Technical standards	New								√		
Guidelines	New								√		
Best practice	New								√		

All participants agreed entirely with the proposed model, except participant 3, who renamed DFR policies to Legal policies.

This was, however, not the only name change to this domain. Not shown on the table was the proposed name change of the entire domain by participants 1, 2, and 6. All three participants opted for Policies and procedures.

Half (five) of the participants moved the Escalation policy element from the Monitor and report domain to the Policy domain. The arguments were that as a policy, it should be moved to the Policy domain.

Participant number 8 argued that a sequence existed between the elements and that the model should be redesigned to reflect this. He suggested the following order: policy at the top, followed by process, procedure, standards and, lastly, guidelines (see Figure 22 that exemplifies his view).

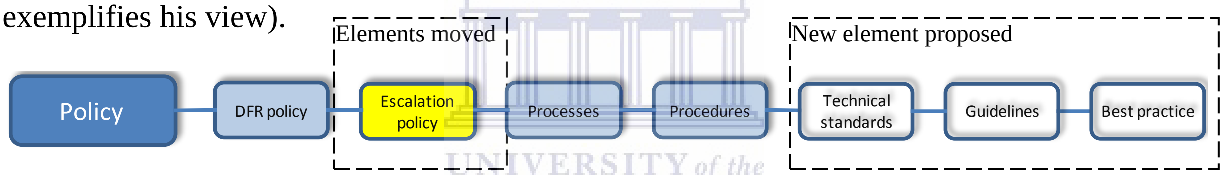


***Figure 22*: Participant 8's view on the Policy domain.**

In summary, the proposed domains were accepted by all participants; however, most added other policy related elements to the domain. The Escalation policy was the element that was added by most of the participant.

Compliance domain

Figure 23 illustrates the proposed Compliance domain model that was presented to the interviewees.

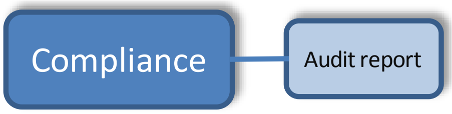


***Figure 23*: Proposed elements of the Compliance domain (Source: Author).**

Table 26 below is a matrix of participant responses to the proposed Compliance domain.

Table 26

Compliance Domain—Matrix of Participant Responses

Element	Type	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10
Audit report	Proposed	√	√			√		√		√	√
Internal audit report	Changed								√		
External audit report	Changed								√		
Regulations	New								√		
Internal fraud combat policy	New									√	√
Compliance report	New									√	√

Most participants agreed with the inclusion of the Audit report element in this domain; however, several changes were desired.

Participants 9 and 10, who are practitioners in the long-term insurance field and whose organisation is in the initial phases of adopting DFR, have included two new elements: Internal fraud combat policy and compliance report. Apart from regulation and legislation compliance, their organisation also requires the forensic unit to comply with its internal fraud combat policy. None of the other participants elected an internal policy. It is possible that other organisations have similar internal policies; however, they understand that this domain is tasked with validating compliance and producing outputs as validation. An element such as an internal fraud combat policy is an input into compliance checking and not an output, unless a separate report is required to form the Compliance domain to feed into the internal combat policy for reporting purposes. But then a name change is advised, from internal fraud combat policy to internal fraud combat report. This would convey the message that this particular report communicates fraud combat non-compliance issues.

Participant 3’s response is not mapped on the matrix as he moved the entire Compliance domain into the Governance domain and thus does not have a separate compliance domain. Similarly, participant 6 moved Compliance to the Legal domain. Participant 4 *did* have a Compliance domain on his model but with no sub-domains underneath it.

Training domain

Figure 24 illustrates the proposed Training domain model that was presented to the interviewees.

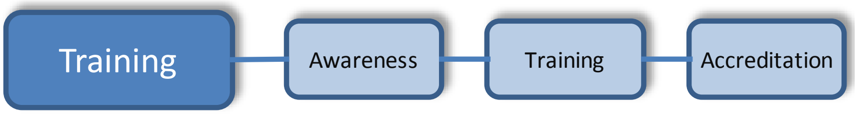


Figure 24: **Proposed elements of the Training domain.**

The matrix in Table 27 below is a representation of participant responses to the proposed Training domain.

Table 27

Training Domain—Matrix of Participant Responses

Element	Type	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10
Awareness	Proposed	√	√	√	√	√	√	√	√	√	√
Training	Proposed	√	√		√	√	√		√	√	√
Accreditation	Proposed			√	√	√	√		√	√	√
Investigative training	Changed			√							
Forensic training	Changed							√			
Forensic accreditation	Changed							√			

The domain is an uncomplicated domain, and the participant responses reflect that. Most (6) agreed completely with the proposed elements, and those that did not opted for clarifying element names. An example is the name change of the Training element to Investigative training by participant 3 or the name change to Forensic training by participant 7. Participant 7 renamed the Accreditation element to Forensic accreditation.

Monitor and report domain

Figure 25 illustrates the proposed Monitor and report domain model that was presented to the interviewees.

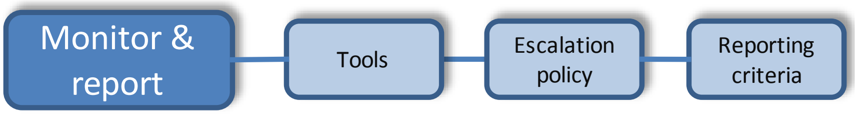


***Figure 25*: Proposed elements of the Monitor and report domain.**

The matrix in Table 28 below is a representation of participant responses to the proposed Monitor and report domain.

Table 28

Monitor and Report Domain—Matrix of Participant Responses

Element	Type	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10
Tools	Proposed				√	√	√	√	√	√	√
Escalation policy	Proposed				√	√		√		√	√
Reporting criteria	Proposed			√		√	√	√	√	√	√
Audit report	Moved	√	√				√				
Monitoring report	Changed			√							
Laboratory accreditation	New			√							
Monitoring requirements	New								√		

Participants 1 and 2 had a dissimilar view to the proposed model. They only included the Audit report element in this domain. The Escalation policy was moved to the Policy domain, based on the DFR checklist that was provided by the participant. This was the only artefact provided by the participants. The artefact is a maturity checklist with particular questions that will enable the organisation to rate its maturity. The artefact is, to a very large degree, a version of the checklist used by Wheeler (2010). The DFR checklist is not an academic document, but it is implemented and utilised by a very large insurance organisation and, as such, was included in this study (see Appendix 4 to examine the checklist).

Domain changes

This study was initiated with eight domains and participants were invited to respond to open-ended questions structured around the proposed domains. However, participants who are forensic practitioners of various industries (see Tables 19 & 20) have suggested domain name changes and the addition of several other domains to the model and hierarchies to the model.

Name changes and additions. Table 29 below shows the domains that have been changed or added by participants. The table shows the old name, new name, new elements in it and the participant who proposed the change. This table is useful for further discussion to unlock the rationale behind the changes and to highlight any new elements that were previously not identified by literature (to be discussed in chapter 6). These elements should be considered when redesigning the DFRCF model and DFR maturity assessment model in answer to the research question.

Table 29

Domain Changes – Based on Participant Responses

Old domain name	New domain name	New sub-domains (elements) introduced	Participant
Policy	Policies & procedures	n/a	P1, P2
Legal requirements	Legal & regulatory	n/a	P1, P2
Legal requirements	Legal requirements & policies	Electronic communications policy	P4
Legal requirements and Policy	Legal compliance	Regulations	P6
Systems & events	Technology	Equipment	P1, P2
Training	Training & education	n/a	P1, P2
n/a	Group support	Exco buy-in	P1, P2
n/a	Lab management	Copies & standard build; Acquisition tool tests; Asset inventory	P1, P2
n/a	Auditing & logging	Forensic findings; Event auditing,	P1, P2
n/a	Public relations & messaging	Fraud awareness; Press statements	P1, P2
n/a	Risk Management	n/a	P4, P5

The proposed name changes are both clarifying in nature and subjective. Examples of this are: Policy to Policies and procedure, Legal requirements to Legal and regulatory or Training to Training and Education.

Group support was re-introduced as a main domain, with Executive buy-in as the sub-domain. Yet executive support is encapsulated in the Strategy domain under DFR strategy, as suggested by literature. However, it could be argued that group support is crucial for large companies and, as such, deserves to be prioritised, something that might not be necessary in small organisations.

Hierarchy within the proposed model. Participant 6, a forensic practitioner in the banking industry, suggested a hierarchy structure based on the Plan, Do, Check, Act cycle. Figure 26 below represents his view.

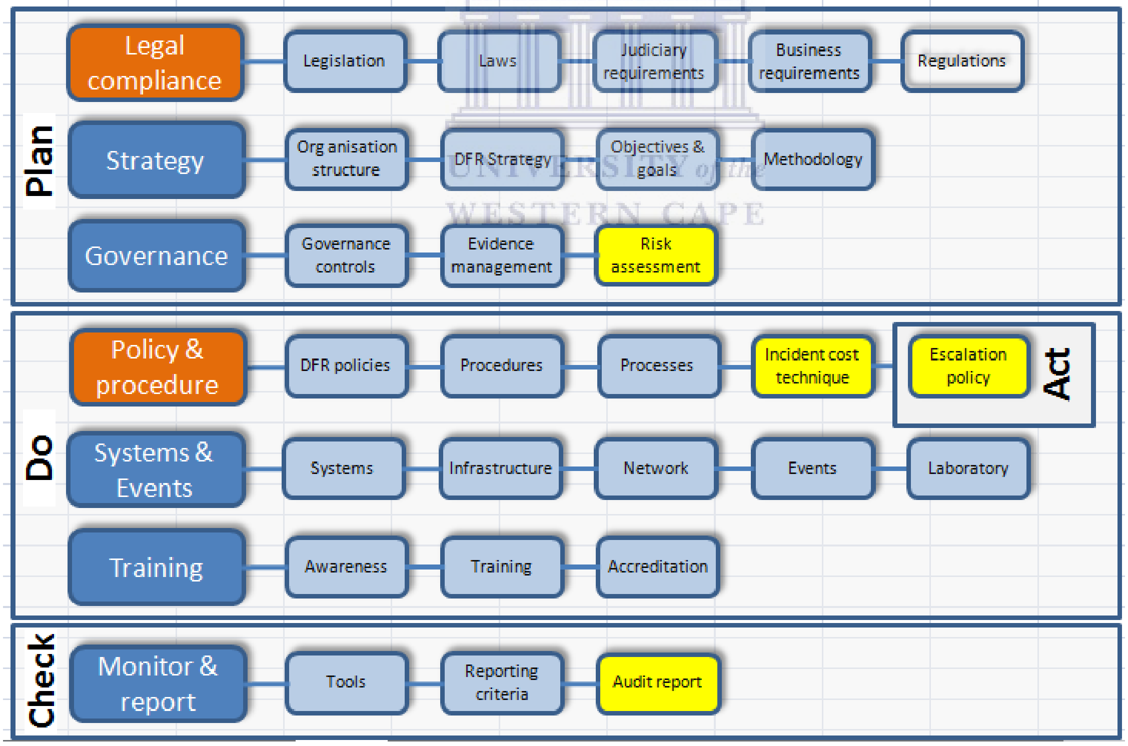


***Figure 26*: Plan, do, check, act cycle hierarchy proposed by participant 6.**

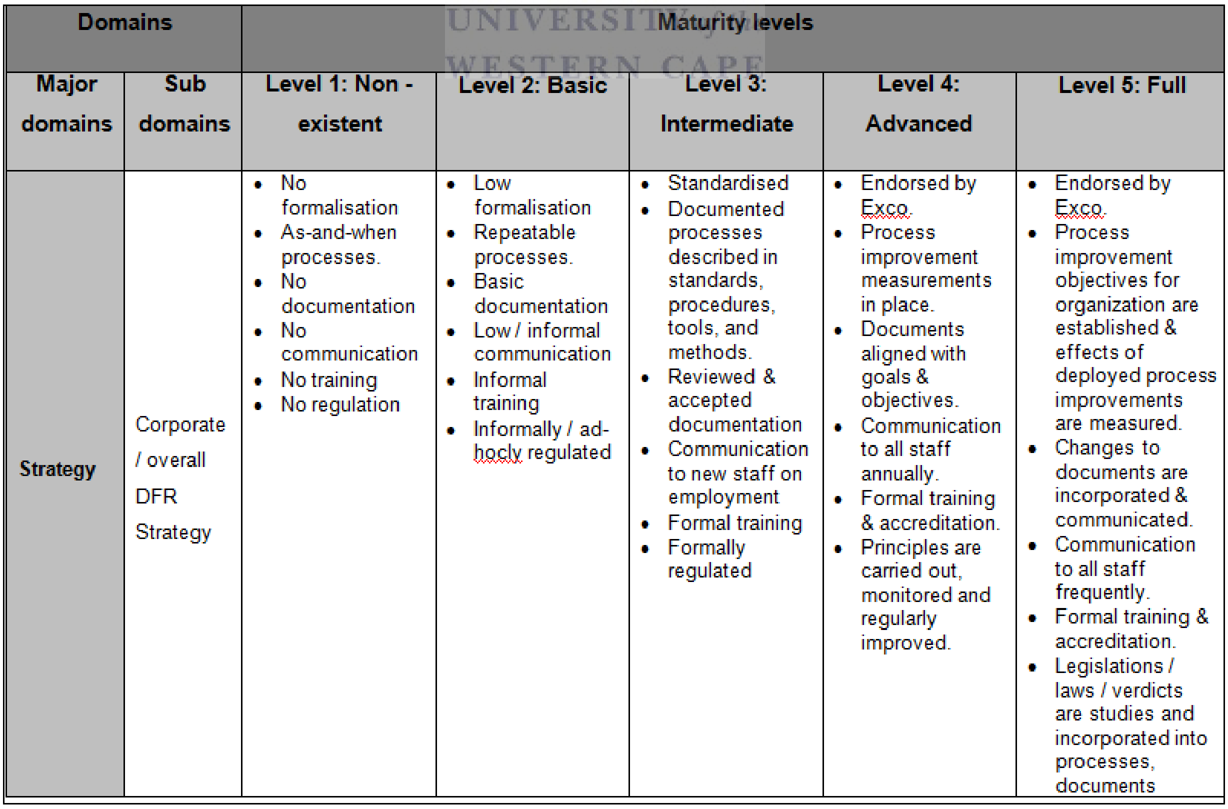
Participant 6 said, "*If you look at any best practice stuff, they usually use those plan, do, check, and act*." The participant was demonstrating that the DFRCF model should be reorganised to represent a cycle of continuous improvement, as a best practice, based on the Deming cycle of continuous improvement.

The cycle is a methodology that is utilised by organisations to continuously improve their products and processes (Deming, 1982).

Digital Forensic Readiness (DFR) maturity assessment model. The objective of the second part of the research question is the utilisation of the DFR structure (domain elements) to design a DFR maturity assessment model is. To enable this, the study must

- Understand whether a checklist approach or a qualitative approach was more appropriate for the assessment model.
- Understand what the descriptions for the maturity levels are.

To fulfil the above two objectives, two maturity assessment models were proposed, and participants were prompted for opinions (see Appendix 2 for the full models). The following are key descriptions of the different approaches and models.



Domains		Maturity levels				
Major domains	Sub domains	Level 1: Non - existent	Level 2: Basic	Level 3: Intermediate	Level 4: Advanced	Level 5: Full
Strategy	Corporate / overall DFR Strategy	• No formalisation • As-and-when processes. • No documentation • No communication • No training • No regulation	• Low formalisation • Repeatable processes. • Basic documentation • Low / informal communication • Informal training • Informally / ad-hocly regulated	• Standardised • Documented processes described in standards, procedures, tools, and methods. • Reviewed & accepted documentation • Communication to new staff on employment • Formal training • Formally regulated	• Endorsed by Exco. • Process improvement measurements in place. • Documents aligned with goals & objectives. • Communication to all staff annually. • Formal training & accreditation. • Principles are carried out, monitored and regularly improved.	• Endorsed by Exco. • Process improvement objectives for organization are established & effects of deployed process improvements are measured. • Changes to documents are incorporated & communicated. • Communication to all staff frequently. • Formal training & accreditation. • Legislations / laws / verdicts are studies and incorporated into processes, documents

***Figure 27*: Approach one: the check-box (tick-box) approach.**

Figure 27 describes the bullet point approach maturity assessment model. The model has two main headings: Domains and Maturity Levels. The domains are the elements that will be assessed on the model and the maturity levels are the matrix against which the domains will be measured. The domains are divided into major domains and sub-domains. The major domain is the high level grouping of related, detailed sub-domains. There are five maturity levels, ranging from level 1 to level 5.

Level 1 is defined as non-existent and it is typically characterised as having no formalisation, no as-and-when processes, no documentation, and so on.

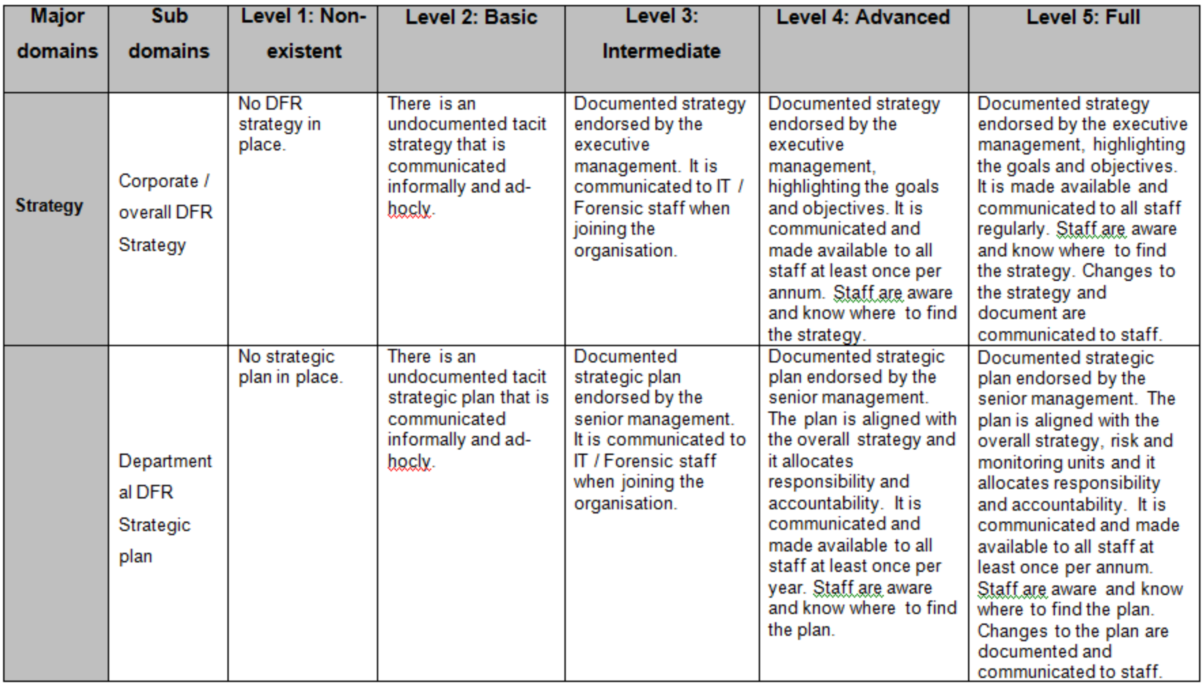
Level 2 is defined as basic and is characterised by low formalisation, repeatable processes, basic documentation, and so on.

Level 3 is defined as intermediate and is characterised as having standardised forensics, documented processes, formal training, and so on.

Level 4 is described as advanced and is typified as having forensics that is endorsed by Executive members, has process improvement measures, and so on

Level 5 is the highest level of the model and is described as full; the characteristics are amongst other continuous process improvement objectives, formal staff training and accreditation, and so on (see Appendix 2 for the full matrix).

Figure 28, below is the second approach: the qualitative approach



Major domains	Sub domains	Level 1: Non-existent	Level 2: Basic	Level 3: Intermediate	Level 4: Advanced	Level 5: Full
Strategy	Corporate / overall DFR Strategy	No DFR strategy in place.	There is an undocumented tacit strategy that is communicated informally and ad-hocly.	Documented strategy endorsed by the executive management. It is communicated to IT / Forensic staff when joining the organisation.	Documented strategy endorsed by the executive management, highlighting the goals and objectives. It is communicated and made available to all staff at least once per annum. Staff are aware and know where to find the strategy.	Documented strategy endorsed by the executive management, highlighting the goals and objectives. It is made available and communicated to all staff regularly. Staff are aware and know where to find the strategy. Changes to the strategy and document are communicated to staff.
	Departmental DFR Strategic plan	No strategic plan in place.	There is an undocumented tacit strategic plan that is communicated informally and ad-hocly.	Documented strategic plan endorsed by the senior management. It is communicated to IT / Forensic staff when joining the organisation.	Documented strategic plan endorsed by the senior management. The plan is aligned with the overall strategy and it allocates responsibility and accountability. It is communicated and made available to all staff at least once per year. Staff are aware and know where to find the plan.	Documented strategic plan endorsed by the senior management. The plan is aligned with the overall strategy, risk and monitoring units and it allocates responsibility and accountability. It is communicated and made available to all staff at least once per annum. Staff are aware and know where to find the plan. Changes to the plan are documented and communicated to staff.

***Figure 28*: Qualitative approach—maturity assessment model.**

Figure 28 describes the qualitative approach to the maturity assessment model. The model is similar to the previous bullet point approach, apart from the level characteristics. All levels are characterised by narrative, descriptive sentences and the model relies on the interpretation of the assessor. The process of rating is a qualitative exercise. The narrative increases with each higher level.

Level 1 – non-existent is characterised by a narrative that describes the absence of the particular element. For example, the domain strategy implies that an organisation needs a corporate/overall DFR strategy. The narrative for level would be "*No DFR strategy in place*".

For *Level 2,* it would be "*There is an undocumented tacit strategy that is communicated informally and ad-hoc*".

For *Level 3,* it would be "*The documented strategy is endorsed by executive management*". This would be communicated to IT/forensic staff when joining the organisation.

This is the trend for the model (see Appendix 2 for the full matrix).

The following open-ended questions were posed to participants to gather the data needed to understand the approach selection: Which maturity assessment model would you prefer and why and how can the maturity levels be further refined to illustrate an escalation from non-existence to full maturity?

Their responses to the selection of the assessment approach were varied, as illustrated by Table 30 below.

Table 30

Responses to the Two Approaches

Approach	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10
Check-box, bullet-point			√	√	√				√	√
Qualitative (words)						√				
Combination approach	√	√					√	√		

Half (5) of the participants preferred the bullet point approach where the subject can tick off a list and understand the maturity level in such a fashion. Participants nine and ten argued that the qualitative approach was too open for various interpretations and the bullet point approach gives them an indication of what is under rating. They also conceded that the selection was based on their level of knowledge of the subject and they would prefer more guidance in implementation then rating. Their organisation is in the early phase of DFR implementation.

Four participants selected a combination of both the qualitative and tick-box approach. This means that a third approach was designed by the participants. This new combination approach was selected by participants in the insurance and private consultancy industries.

Participant 6, from the banking industry, was the only respondent, who opted for the qualitative approach, saying, "*People come with a check list mentality. Then you will say I do have this I have some of that but there will always be something missing*". The participant argued that the check-box approach stifles out-of-the-box thinking and thus will cause information to be overlooked.

Below are all the participant's rationales for accepting or rejecting the bullet point approach (see Table 31).

Table 31

Responses to the Check-Box Approach

In support	Against	Participant
Gives indication of what needs to be addressed.		P9, P10
It is easier.		P5
It is fleshed out nicely. It gives you a roadmap.		P4
It is a standard way of assessing maturity. More clearly stated than the other approach. It fits in with other models.		P3
	Assessors will have a checkbox mentality and not think outside the box. It will overlook information. You will get wrong answers.	P6
	Definitions/bullet points are problematic as they can create overlaps. Levels must be aligned and show clear ascension.	P8
Nice tick box and auditors love this. It is easy to determine levels. More comprehensive then qualitative approach. For people who are new to forensics.	*It can't be used across industries.*	P7
You can do self-assessments		P1, P2

Below are all the participant's rationales for accepting or rejecting the qualitative approach (see Table 32).

Table 32

Responses to the Qualitative Approach

In support	Against	Participan
	Too open for different interpretations	P9, P10
It is a better approach. It is based on a feeling that we have. It is subjective.		P6
	Too easy to move up a level.	P8
It is more generic	*A lot more difficult to monitor. Requires very skilled assessors. More for skilled people.*	P7

In summary, the semi-structured interviews were instrumental in collecting data relating to DFR structure (domains and sub-domains) and the assessment matrix. The overall objective of the study, as encapsulated in the research question, "*What DFR structure (components or domains) is needed by financial services businesses, and how can such a structure contribute to the design of a maturity assessment model that satisfies the goals and objections of DFR?"* was met by the data collection process.

The data collection process uncovered that half of the participants preferred the check-box (tick-box) approach and four participants selected a combination of the two approaches. Only one participant felt that the qualitative approach was preferred. None of the participants rejected or offered alternative maturity levels.

Chapter Summary

This chapter illustrated the results of the interviews with forensic practitioners. Several key changes were communicated by the participants. A demographic was also compiled to understand the participant's level of influence in the digital forensic environment. In the next chapter, the results of the interviews will be discussed in detail.

CHAPTER 6: DISCUSSION, CONCLUSION & RECOMMENDATIONS

This chapter presents the findings of the research study. In it, conclusions are drawn and suggestions and recommendations made for future research.

Discussion of Findings

This study was intended to investigate the structure that is necessary to implement digital forensic readiness and how such a structure might be useful in the design of a maturity assessment model. To achieve this, the existing DFR frameworks were analysed and the DFRC framework extended according to the findings of the analysis. The structure of the extended DFRCF was utilised to design a DFR maturity assessment model.

The maturity assessment model and domains were refined through interactive semi-structured interviews with forensic practitioners. The findings from the interviews were presented in Chapter 5. In the following subsection, the DFR domains are discussed.

DFR Domains (Structure)

Strategy

The purpose of this domain is to select a methodology for evidence collection, an organisation structure that reflects the reporting lines of the forensic unit, a forensic strategy, buy-in from executive level, and business requirements that reflect the goal and objectives of the organisation (Grobler et al., 2010b).

The above objectives are best encapsulated by Figure 29 and so this revised model is the final version of the domain.

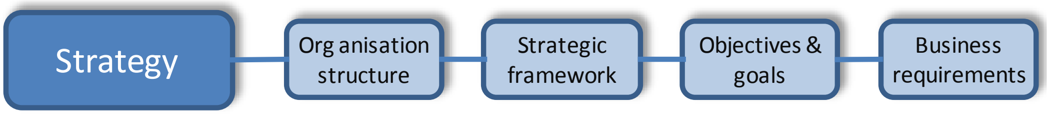


***Figure 29*: Strategy domain and elements (Source: Author).**

The union of the DFR strategy and Methodology sub-domains was a sound decision. As mentioned by participants 1 and 2, not all organisations have a specific DFR strategy, but they most likely will have a forensic strategy or another strategy that addresses the same issues. The use of the term DFR was too specific so was elevated to make it more generic. The use of the words *strategic framework* implies strategy, method, and, better yet, a framework in which evidence will be collected, based on a strategic mandate.

Legal

Although this domain evoked a wide range of responses, it highlighted a very consistent focus on compliance to laws, legislation, and regulations. The conversations resulted in the disentanglement of the above three terms. The above three terms were terms that were applicable to other countries and not entirely relevant in the South African context. *Legislation* was renamed *Statutory laws*, *Laws* was renamed *Common law*, and *Judicial requirements* were renamed *Case law*.

Participants 1 and 2 suggested the renaming of the domain to Legal and regulatory. The argument was that organisations must not only consider laws but must also consider regulations, such as the electronic communications policy or the Payment Card Industry Data Security Standard (PCIDSS). The PCIDSS is a security standard by which organisations abide to ensure maximum security for online credit card transmissions (PCI, 2013). Therefore, a decision was made, for this study, to extend the sub-domains by including a Regulation sub-domain and changing the domain name to Legislation and regulation (Figure 30). One participant suggested the amalgamation of Legal and Compliance. Although these two domains seem to examine the same set of information (laws), they must remain separate as they have dissimilar focus points. The Legal domain ensures that business requirements and the DF strategy are considering legislative issues for implementation. Compliance focuses on examining the extent to which an organisation has fulfilled the requirements of practices and legislation (Bonanzi et al., 2010).

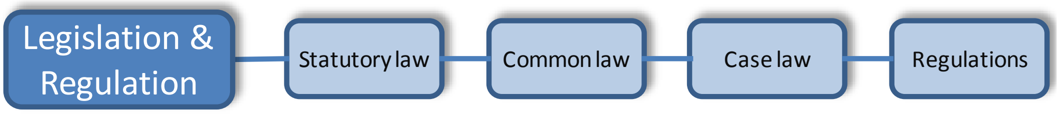


Figure 30: **Legislation and regulation domain and elements.**

Governance

The domain ensures that an organisation establishes DF policy frameworks and that the policies and policy frameworks are implemented according to agreed standards. The Incident cost techniques element was renamed to *Incident management*. The previous name was too granular and conveyed the understanding that the cost technique was the only item under discussion. Participants suggest that there are more underlying activities such as *what, how* and *when* one is going to deal with incidents.

This study has extended the Governance domain and the final version is depicted in Figure 31.

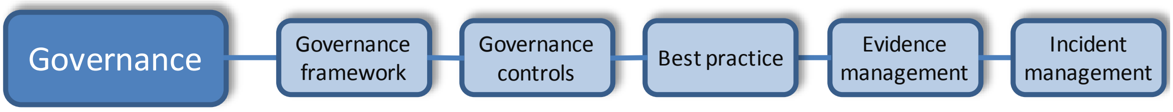


Figure 31: **Governance domain and elements.**

Systems and events

The domain ensures the classification of hardware, software, processes, and events that house potential evidence. Moreover, as Rowlingson (2004) noted, this domain ensures that a risk assessment is performed at business level. The prevailing sentiment among participants was that Infrastructure, Network, Systems, Events and Laboratory must remain within the domain.

Participant 7 suggested that the Systems element be divided into three separate sub-domains: *Technological systems*, *Organisation systems* and *Workflow systems*. The proposed name changes will be overlooked by this study because it is possible that other types of systems are in use in different organisations and the grounds for the particular breakdown this study have not been established. However, the suggestion to rename Laboratory to DF capacity was accepted as prudent for this study. As mentioned earlier, this domain seeks to ensure that there is some form of forensic ability and skill, rather than a facility.

This study has extended the Systems and events domain and the final model is depicted in Figure 32.

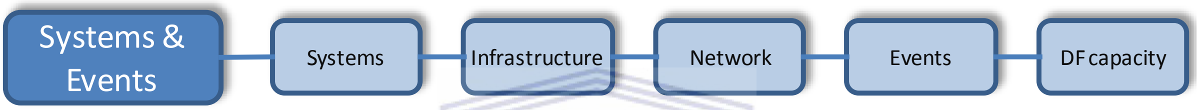


***Figure 32*: Systems and events domain and elements (Source: Author).**

Policy

Policies that guide user behaviour within an organisational context must be established. Various policies are applicable to DFR (Barske et al., 2011), as mentioned in Chapter 3 of this study.

Table 33 illustrates all the elements proposed in this study. They have been grouped to show compatibility and ease of reference.

Table 33

Systems and Events Domain and Elements

Policy	Procedure	Process	Standards	Guideline	Best practice
DFR policy	Procedure	Process	Technical standards	Guidelines	Best practice
Escalation policy	Incident cost technique	Reporting process			
Evidence management policy					
Legal policy					
E-comms policy					
Incident management policy					

It is impractical to display the level of detail as proposed by the various responses into a single model, especially since all the elements can be described by meaningful groupings. As an example, under the Policy grouping, it becomes clear that all the elements listed underneath it are policies, but with varied focuses, and it is thus efficient to refer to all the different polices as *Policy*.

This study will utilise the above groupings to populate the Policy domain.

See Figure 33 below for the final refined model.

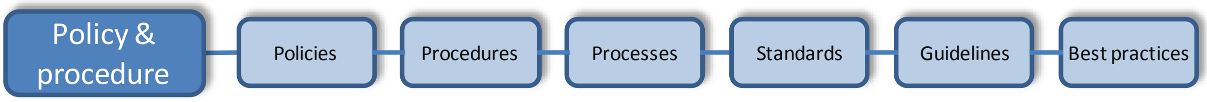


***Figure 33*: Policy and procedure domain and elements.**

Compliance

The element of compliance does not feature strongly in previously published literature, and the few times it is mentioned, it is mentioned in the context of staff adherence towards policies and not as a separate element that assesses the effectiveness of controls. This means there might be a policy, and staff might adhere to it, but no effective controls exist to measure it against the IT objectives.

Grobler et al. (2010a) introduced the discussion around control measures, and participants' responses indicate a need for a separate focus on this element. All participants agreed that there must be a Compliance main domain, but it was participants 3 and 6 who preferred that Compliance be treated as a sub-domain.

Participant 3 proposed that the Compliance domain reside within the Governance domain; however, this study has already demonstrated the need to keep these two domains separate (see Chapter 0).

Participant 6 argued that the Compliance element should move to the Legal requirements domain. As mentioned, compliance has a separate focus, that is, measuring the controls put in place, and this cannot reside within a legal context.

The interpretation that regulations should be considered within this domain was not expressed by other participants, except by participant 8, who argued that compliance should ensure that an organisation complies with laws and regulations. However, in this study, it is argued that the objective of the Compliance domain is not to re-evaluate conformance to legal requirements: this is already performed within the Legal requirements domain.

The final refinement to this domain is shown in Figure 34. The Audit element refers to internal audits and external audits. The compliance report is an output of the audit investigation. Typically an audit would be performed to check company compliance to policy, procedure and legislation (Bonanzi, et al., 2010). After which a report (compliance report, audit report, findings report, or whatever the organisation decides to name it) would be produced (Kochan, 1993). This study did not use audit reports as most people view audit reports as documents that are prepared by external parties and professionals (Auditors) and as such would not see that it can also refer to a report generated by a compliance officer. Compliance report refers to any type of report generated after an audit was performed, irrespective if it was performed by professionals (Auditors) or non-professional (Compliance officer, administrative staff).

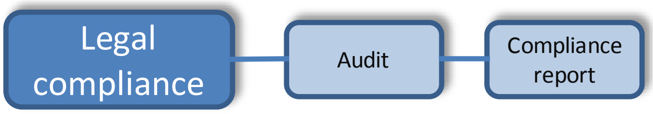


***Figure 34*: Compliance domain and elements.**

Training

The Training domain is uncomplicated and all participants accepted the proposed model. There were two suggestions to rename Training as Forensic training and Investigative training. Another opinion was to rename Accreditation as Forensic accreditation.

The Training element will be renamed Forensic training and the Accreditation element will remain as such because accreditation in this regard not only refers to forensic accreditation but also to laboratory accreditation. Laboratory accreditation is becoming more evident in later research. See Figure 35 for the final refinement in this domain.

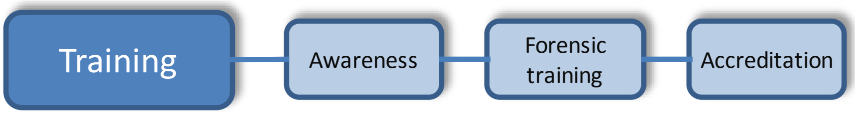


***Figure 35*: Training domain and elements (Source: Author)**

Monitor and reporting

This completion of this domain elicits the organisation's incident response reports, reporting criteria, and the tools to perform intrusion detection, and it ensures the organisation understand their requirements for how the IDS triggers must function. It also ensures that the organisation develops standards to guide the interaction between affected individuals (Jordaan, 2009; Rowlingson, 2004).

An initial proposal in this study was to include the Escalation policy in this domain; however, half of the respondents felt that an escalation policy must reside within the realm of policies and therefore the Escalation policy was removed from this domain and moved to the Policy domain. However, this left a gap as this domain required an action that ensures that there is an escalation as certain incidents must be forwarded for formal investigations, based on the triggers created. However, this escalation is not aimed at any procedure but rather at answering the questions: *when must we escalate* (when) and if these requirements are met, *what then* (what to do)? This *when* and *what* will be answered by an element named *Escalation criteria*. The Escalation criteria sub-domain will effectively create the link between *what* and *when* (escalation criteria) and *how* (escalation policy).

Figure 36 illustrates the refined elements of the domain.

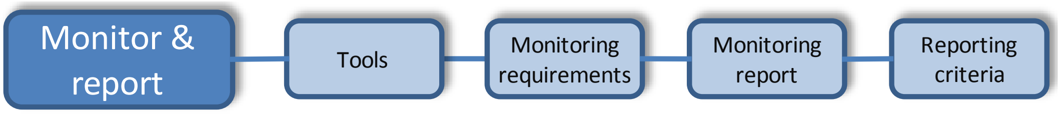


***Figure 36*: Monitoring and reporting domain and elements (Source: Author).**

Cycle

Although only one participant proposed a cyclical structure, it is apparent that such a structure will assist start-up organisations in organising themselves and prioritising pieces of work. The implementation of DFR should be incremental as the organisation continues to mature.

The proposed hierarchy is based on the Deming cycle of continuous process improvement (Deming, 1982). The four steps in the Deming cycle are:

- Plan—planning the process of DFR.
- Do—acting on the process.
- Check— measuring the outcomes by discovering insufficiencies.
- Act—acting on the gaps between target and achieved outcomes.

The DFRCF-v2 will incorporate the Deming approach by illustrating where the domains are affected by the Deming cycle.

Overall DFRCF Model

Initially, eight domains (as part of the extended DFRCF-v1) were proposed, and post interviews had five new domains added to the model. The new domains and new sub-domains are reflected in Table 34.

Table 34

New Domains and Elements Suggested by Participants

New Domain name	New sub- domains (elements) introduced	Participant
Group support	Exco buy-in	P1, P2
Lab management	Copies and standard build; Acquisition tool tests; Asset inventory	P1, P2
Auditing & logging	Forensic findings; Event auditing;	P1, P2
Public relations & messaging	Fraud awareness; Press statements	P1, P2
Risk Management	n/a	P4, P5

The main objectives of Group support are to ensure that DF receives the high level support from senior members of the organisation needed to ensure that budgets are allocated and that prioritisation is encouraged. However, the initial proposed model made the executive support part of the DFR strategy element. The organisation that proposed the new domain is a very large international organisation and.it is understandable to see a separate focus for executive support. However, smaller organisations do not have the complex management hierarchy that the very large corporates have and so, in this study, the initial proposal to include Executive support as part of the DFR strategy is supported.

The above argument also applies to the proposed Auditing and logging and Public relations and messaging. The two new proposals do not warrant a focus as separate domains.

The same argument holds true for the proposed Lab management. It will remain part of the Systems and Events domain. Further, as participant 7 (the most respected practitioner in the sample) reiterated, “*They only set out rooms for laboratories in large companies and this is to test capacity not facilities”*. Moreover, the sub-domains proposed under the Lab management domain are too low-level (detailed). The model must remain consistently medium-level (between high-level and low-level of detail).

Risk management is an important aspect within any business and as such deserves a separate focus. The domain will remain Risk management.

The final main domains are illustrated in Figure 37 below:

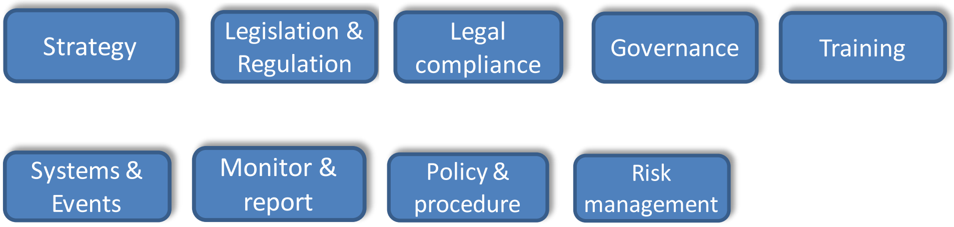


***Figure 37*: Refined domains of DFRCF (Source: Author).**

Maturity Assessment Model

For this study, the check-list approach model (see Table 36) was accepted as the final DFR maturity assessment model. The model visualises an approach that will assist organisations to assess their maturity levels. As earlier stated, this model is a prescriptive model as organisations can utilise it to plot a path towards higher maturity. The maturity levels were defined with the input of the forensic practitioners, thus strengthening the validity of the approach followed to define the maturity levels.

How to read and complete the assessment model

The *domains* entity on the model illustrates which domains and sub-domains are applicable in relation to the *maturity level*. The domain field is left unpopulated in Table 35—this is to illustrate that the maturity levels are applicable to each/every/any domain and sub-domain. There are 5 levels of maturity in the model, which should be read from left to right, in a horizontal line.

To achieve a rating of, for example, Level 2, the organisation has to comply with all the conditions mentioned under Level 2–Basic. If all the conditions have not been met, then the score will be lowered to the previous level, which is Level 1–non-existent. This trend should be followed consistently for all the levels, except for Level 1, since there is no level lower then Level 1.

Table 35

DFRCF Maturity Assessment Model

Domains		Maturity levels				
Major domain	Sub domain	Level 1: Non - existent	Level 2: Basic	Level 3: Intermediate	Level 4: Advanced	Level 5: Full
		• No formalisation • As-and-when processes. • No documentation • No communication • No training • No regulation •	• Low formalisation • Repeatable processes. • Basic documentation • Low / informal communication • Informal training • Informally / ad-hocly regulated	• Standardised • Documented processes described in standards, procedures, tools, and methods. • Reviewed & accepted documentation • Communication to new staff on employment • Formal training • Formally regulated	• Endorsed by Exco. • Process improvement measurements in place. • Documents aligned with goals & objectives. • Communication to all staff annually. • Formal training & accreditation. • Principles are carried out, monitored and regularly improved.	• Endorsed by Exco. • Process improvement objectives for organization are established & effects of deployed process improvements are measured. • Changes to documents are incorporated & communicated. • Communication to all staff frequently. • Formal training & accreditation. • Legislations / laws / verdicts are studies and incorporated into processes, documents

Conclusion

Organisations that do not have a means to measure their forensic readiness run the risk of economic crime exploitation. This study examined current literature to understand what the DFR structure is and how such a structure can be used to design a maturity assessment model.

The structure became apparent from an analysis of previously published literature and a qualitative approach was used to test the DFR structure with forensic practitioners. The respondents shaped the structure (domains) and the domains were used to create a maturity assessment model. Two approaches were proposed to participants, however, a third response, which is a combination of check list and qualitative narration, was also proposed by the respondents.

Extended DFRCF Model V2–Post-Participant Input

The final structure (domains and sub-domains) are illustrated in Figure 38 below. The figure demonstrates the scope and structure of DFR and is thus useful to financial services organisations that invest in DFR. The figure illustrated is the extended DFRC-v2 framework—after it has been tested in the real world—and it mimics the Deming lifecycle: Plan, Do, Check and Act. This is the final product of the extended DFRCF in this study and this tested framework is introduced to the academic world and to the forensic practitioners.

This framework will allow organisations to implement and manage their DFR programmes as it illustrates the scope of DFR and it achieves the goals and objectives of DFR, as postulated by the various literary works shown in Table 1 of this study. Thus, the post-alignment of some activities, such as the alignment of business goals to forensic goals and the alignment of business risk units with incidents monitoring units, will be avoidable (Whyte & Claims, 2012).

However the DFRCF-v2 is still a theoretical framework that must still be tested in practice – before generalisation of the framework (Karokola, Kowalski & Yngström 2013).

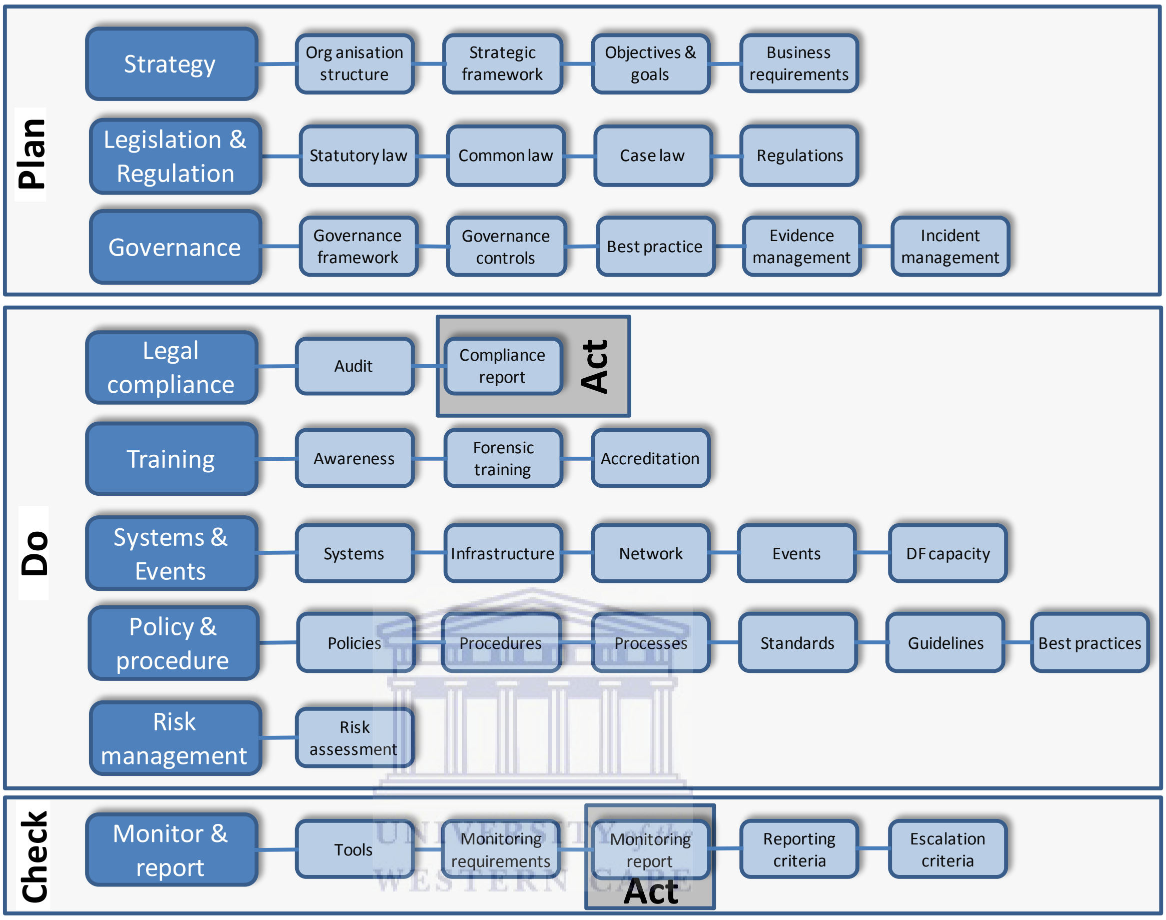


***Figure 38*: DFRCF-v2—post practitioner input.**

DFR Maturity Model

There was a sufficient split in the responses of the participants when deciding which maturity model to use. Five participants preferred the check-list approach, one participant preferred the qualitative approach, and the remaining four favoured a combination of the two approaches. The check-list approach was elected, as the majority of the participants were in favour of this model.

The final DFR maturity assessment model is illustrated by Table 35. This model is the first step towards calculating a maturity score. It is important for organisations to understand their forensics readiness capability as this will enable them to achieve and remain in a state of true forensic “readiness”. An organisation that knows its readiness status is in a better position to manage and implement interventions that are aimed to achieve a maturity rating of *5*.

However, the DFRMAM is still a theoretical model and its practicality must still be tested in the real world—before generalisation of the model.

Summary

The study understood that financial services organisations do not have access to non-proprietary assessment models to measure the DFR, furthermore, organisations that do perform DFR assessments, utilise frameworks that do not exclusively satisfy the goals and objectives of DFR.

To resolve this problem the study interrogated existing DFR frameworks to understand their structure (domains and sub domains). This interrogation led to the amendment of the DFRC framework. This process effectively resolved the second question of the research.

Having understood the structure, the study investigated the goals and objectives of DFR to ensure that the extended DFRCF exclusively satisfies the goals and objectives of DFR. This effectively resolved the first question of the research.

The study investigated maturity assessment models to understand if they can be utilised to assess DFR. The study found that none were suitable for this purpose and as such the study developed a maturity assessment model utilising the design principles. This effectively resolved the third and last (fourth) research questions.

The study further tested the extended DFCRF and the DFR maturity assessment model by conducting semi-formal interviews with forensic practitioners. The final DFRCF mimics the Deming lifecycle in the fact that it has Plan, Do, Check and Act phases. This approach is not prevalent in existing literature. The strength of this framework is that it meets the goals of DFR, is modelled on the Deming cycle and has had a first iteration with forensic experts. The model is re-usable across industries such as banks, insurance and forensic houses. The weakness of this framework is that it has not been extensively tested in the real world. Also, a better approach for data collection would have been a focus group, but as mentioned in the study this was not feasible due to time and budget constraints.

The study proposed two approaches to the maturity assessment model, namely a bullet point approach and a qualitative approach. Most of the participants selected the bullet point approach. The participants also suggested a new approach, namely, a combination of the bullet and qualitative approach. The weakness of the chosen bullet point model is that it requires a questionnaire or checklist to guide in the calculation of a maturity level.

All in all the research has answered its research questions and thus resolved the main problem.

Recommendations for Future Research:

In this study, the structure needed for DFR was investigated and how such a structure can contribute to the design of a maturity model was also examined. Both of these objectives have been met by this study; however, the maturity assessment model alone cannot sufficiently provide a maturity assessment. This study proposes that future research focus on designing a checklist, as mentioned in Appendix 4, to aid in the calculation of the maturity level. It is also recommended that practitioners and/or academics test both the DFRCF-v2 and the DFRMAM in practice—before generalisation (Karokola et al., 2013).

Future research should seek to test the DFRCF extensively in the real world and should consider developing a combination maturity assessment model, as suggested by this study.

REFERENCES:

Altrichter, H., Kemmis, S., McTaggart, R. & Zuber-Skerritt, O. (2002). The concept of action research, *The Learning Organization*, 9(3), 125 – 131.

Amaratunga, D., Baldry, D., Sarshar, M. & Newton, R. (2002). Quantitative and qualitative research in the built environment: application of "mixed" research approach, *Work Study, 51*(1), 17-31. doi:10.1108/00438020210415488

Barske, D., Stander, A., & Jordaan, J. (2010,). *A Digital Forensic Readiness Framework for South African SME's*, Proceedings of the Information Security for South Africa, pp. 1-6, Johannesburg, RSA, 2-4 August, 2010

Becker, J., Knackstedt, R. & Pöppelbuß, J. (2009). Developing maturity models for IT management—A procedure model and its application. *Business & Information Systems Engineering (BISE), 1*(3), 213-222. doi:10.1007/s12599-009-0044-5

Bonazzi, R., Hussami, L., & Pigneur, Y. (2010). Compliance management is becoming a major issue in IS design. In *Information Systems: People, Organizations, Institutions, and Technologies*, pp. 391-398). Heidelberg, Germany: Physica-Verlag HD.

Bradford, P., Brown, M., Perdue, J., & Self, B. (2004, 5-7 April). *Towards proactive computer-system forensics, Proceedings* of the Information Technology: Coding and Computing, ITCC .pp. 648-652.

Brown, W., Moore, G. & Tegan, W. (2006). *Effective governance through the IBM SOA Governance Management Method approach*. White paper. 2006. Retrieved from https://play.petalslink.org/download/attachments/3050038/gov-ibm.pdf

Business Week. (2009). The most innovative companies 2009, 2009. Retrieved from http://www.businessweek.com.

Casey, E. (2004). *Digital evidence and computer crime* (2nd ed.). Cambridge, MA: Elsevier Academic Press.

Charmaz, K. (2007). T*he Sage handbook of grounded theory*. Thousand Oaks, CA: Sage.

Cooper, D. R. & Schindler, P. S. (2001). *Business research methods*. New York, NY: McGraw-Hill.

Corbetta, P. (2003). *Social research: Theory, Methods and Techniques Paradigms of Social Research*. London: Sage.

Creswell, J. (2003). *Research design: Qualitative, quantitative and mixed methods approaches* (2nd ed.). Thousand Oaks, CA: Sage.

Creswell, J. W. (2007). *Qualitative inquiry and research design: Choosing among five traditions* (2nd ed.). Thousand Oaks, CA: Sage.

Danielsson, J. & Tjostheim, I. (2004). *The Need for a Structured Approach to Digital Forensic Readiness*. Proceedings of the International Association for Development of the Information Society, pp. 417-421, Lisbon.

De Bruin, T., Freeze, R., Kaulkarni, U. & Rosemann, M. (2005). *Understanding the main phases of developing a maturity assessment model*. Australasian Conference on Information Systems, Sydney, 30 November-2 December 2005.

Deming, W. .E. (1982). *Out of the crisis*. Boston, MA: MIT Center for Advanced Engineering Study.

Dilley, P., (2004). Interviews and the philosophy of qualitative research. *The Journal of Higher Education*. *75*(1), 127-132. doi.org/10.1353/jhe.2003.0049

Dobson, P. J. (2000). Critical realism and information systems research: Why bother with philosophy? *Information Research*, *7*(2). Retrieved from http://InformationR.net/ir/7-2/paper124.html]

Financial Services Board of South Africa. (2010). *List of registered insurers*. Retrieved from http://www.fsb.co.za/Magic94Scripts/mgrqispi94.dll?APPNAME=Web&PRGNAME =List_Of_Registered_Insurers

Flick, U. (2011). *Introducing research methodology: A beginner's guide to doing a research project*. London, UK: Sage.

Fraser, P., Moultrie, J., & Gregory, M. (2002). *The use of maturity models/grids as a tool in assessing product development capability.* Proceedings of the IEEE International Engineering Management Conference, pp. 244-249. Cambridge: UK. doi:10.1109/IEMC.2002.1038431

Gable, G. G. (1994). Integrating case study and survey research methods: an example in information systems. *European Journal of Information Systems,* 3(2), 112-126.

Geertz, C. (1973). The interpretation of cultures: Selected essays. New York, NY: Basic Books.

Gelo, O., Braakmann, D. & Benetka, G. (2008). Quantitative and qualitative research: Beyond the debate. *Integrative Psychological and Behavioral Science, 42*(3), 266-290. doi:10.1007/s12124-008-9078-3

Goddard, W. & Melville, S. (2004). *Research methodology: An introduction* (2nd ed.). Cape Town, RSA: Juta.

Grandison, T., Bilger, M., O’Connor, L., Graf, M., Swimmer, M., Schunter, M., Wespi, A. & Zunic, N. (2007). Elevating the discussion on security management: The data centric paradigm. *Proceedings of the 2007 2nd IEEE/IFIP International Workshop on Business-Driven IT Management (BDIM),* 21 May 2007, pp. 84-93.

Grobler, C. P., Louwrens, C .P. & Von Solms, S. H. (2010a). A framework to guide the implementation of Proactive Digital Forensics in organisations, *Proceedings of the '10*

International Conference on Availability, Reliability, and Security (ARES), Krakow, 15 February -18 February, pp. 677-682.

Grobler, C. P., Louwrens, C. P. & Von Solms, S. H. (2010b). A multi-component view of digital forensics. *Proceedings of the '10 International Conference on Availability, Reliability, and Security (ARES)*, Krakow, 15 February -18 February, pp. 647-652.

Gummesson, E. (1999). *Qualitative methods in management research*. (2nd ed.), London., UK: SAGE,

Henderson, J. C. & Venkatraman, N. (1993). Strategic Alignment: Leveraging Information Technology for Transforming Organizations, *IBM Systems Journal*, *32*(1). doi:10.1147/sj.382.0472

Hillman, P. (1994). *Making self-assessment successful*. *The TQM Magazine*, *6*(3), 29-31.

Jankowicz, A. D. (2000). *Business research projects for students*, (2nd ed.). London, UK: Chapman and Hall.

Johnson, R. B. & Onwuegbuzie, A. J. (2004). Mixed methods research: A research paradigm whose time has come. *Educational Researcher*, *33*(7), 14-26. doi:10.1108/09544789410057863

Johnson, R. B., Onwuegbuzie, A. J. & Turner, L. A. (2007). Toward a Definition of Mixed Methods Research . *Journal of Mixed Methods Research*, 1(2), 112-133. doi:10.1177/1558689806298224

Jonker, J. & Pennink, B. (2009), The essence of research methodology – a concise guide for Master and PhD students in Management Science, New York, NY: Springer.

Jordaan, J. (2009). *The case for digital forensic readiness*, University of Cape Town, Unpublished paper.

Karokola, G., Kowalski, S., & Yngström, L. (2013). Evaluating a Framework for Securing e-Government Services—A Case of Tanzania. *Proceedings of the 2013 46th Hawaii*

International Conference on System Sciences, Johannesburg, South Africa, ISBN: 978-1- 4577-1482-5.

Kelliher, F. (2005). Interpretivism and the Pursuit of Research Legitimisation: An Integrated Approach to Single Case Design. *The Electronic Journal of Business Research Methodology,* 3(2), 123-132.

Kochan, A. (1993). Internal evaluations. *The TQM Magazine,* 5(2).

Kohn, M., Eloff, J. H. P. & Olivier, M.S. (2006). Framework for a digital forensic investigation. *Proceedings of the ISSA 2006 from Insight to Foresight Conference*, Sandton, South Africa, 5-7 July 2006, ISSA, Pretoria, South Africa, ISBN 1-86854-636-5.

Kuo, C., Dunn, K., & Randhawa, S. (1999). A case study assessment of performance measurement in distribution centers. *Industrial Management & Data Systems, 99*(2), doi:10.1108/02635579910261068

Luftman, J. N., Lewis, P.R. & Oldach, S. H. (1993). Transforming the enterprise: The alignment of business and information technology strategies. *IBM Systems Journal, 32*(1).

Mack, N., Woodsong, C., Macquee, K., Guest, G., & Namey, E. (2005). *Qualitative research methods: A data collector's field guide*. Retrieved from www.fhi.org

Mackenzie, N. & Knipe, S. (2006). Research dilemmas: Paradigms, methods and methodology. *Issues In Educational Research*, 16(2), 193-205. http://www.iier.org.au/iier16/mackenzie.html

Maier, A. M., Moultrie, J., & Clarkson, P. J. (2009). Developing maturity grids for assessing organisational capabilities: Practitioner guidance. *Proceedings of the 4th International Conference on Management Consulting, Academy of Management (MCD*), Vienna, Austria, 11–13 June 2009.

Miles, M. B., & Huberman, A. M. (1984). *Qualitative data analysis*. Thousand Oaks, CA: Sage.

Minnesota Historical Society. (1996). *Transcribing, editing and processing oral histories* (Oral History Association of Minnesota, 1996). Retrieved from http://www.mnhs.org/collections/oralhistory/ohtranscribing.pdf

Palmer, G. (2001). A road map for digital forensic research. *Report from the First Digital Forensic Research Workshop (DFRWS),* Utica, New York

Pangalos, G., Ilioudis, C., & Pagkalos, I. (2010). The importance of corporate forensic readiness in the information security framework. *Proceedings of the 2010 19th IEEE International Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE),* Larissa, 28-30 June 2010, pp. 12-16, 978-1-4244-7216-1.

Pangalos, G. & Katos, V. (2010). Information Assurance and Forensic Readiness. *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, 26,* pp. 181-188.

Payment Card Industry. (2013). PCI Standards and Documents. Retrieved from https://www.pcisecuritystandards.org/security_standards/documents.php?document=pci_dss_v2-0#pci_dss_v2-0

Peters, S. (2009). *2009 CSI Computer Crime and Security Survey*. http://gocsi.com/sites/default/files/pdf_survey/CSI%20Survey%202009%20Comprehensive%20Edition.pdf (Accessed 10 September 2013).

Pöppelbuß, J. & Röglinger, M. (2011). What makes a useful maturity model? A framework of general design principles for maturity models and its demonstration in business process management. *Proceedings of the 19th European Conference on Information Systems (ECIS),* Helsinki, Finland.

Pricewaterhousecooper.(PWC) (2011). *Global Economic Crime Survey 2011 (GECS).* Retrieved from www.pwc.co.za/crimesurvey

Raber, D., Winter, R., & Wortmann, F. (2012). Using quantitative analyses to construct a capability maturity model for business intelligence. *Proceedings of the 2012 45th Hawaii International Conference on System Sciences*, Maui, Hawaii, 4-7 January 2012, pp. 4219-4228. doi:10.1109/HICSS.2012.630

Ramirez, T. M. (2002). *You can't manage what you don't measure. Measuring project performance*. Retrieved from http://www.pmipr.org/html/Presentaciones/You%20Cant%20Manage%20What%20You%20Dont%20Measure.pdf

Randeree, K., Mahal, A., & Narwani, A. (2012). A business continuity management maturity model for the UAE banking sector, *Business Process Management Journal*, *18*(3), 5. doi:10.1108/14637151211232650

Reason, P., & Bradbury, H. (Eds.). (2001). Handbook of action research: Participative inquiry and practice. Sage.

Röglinger, M., Pöppelbuß, J., & Becker, J. (2012). Maturity models in business process management, Business Process Management Journal, *18*(2), 328-346. doi.org/10.1108/14637151211225225

Rowlingson, R. (2004). A ten step process for forensic readiness. *International Journal of Digital Evidence*, *2*(3), 1-28.

Sarbanes-Oxley (SOX). (2013). The Sarbanes-Oxley Act. Retrieved from http://www.sox-online.com

Solli-Sæther, H. & Gottschalk, P. (2010). The modelling process for stage models. *Journal of Organizational Computing and Electronic Commerce*, *20*(3), 279-293. doi:10.1080/10919392.2010.494535

Soni, G. & Kodali, R. (2013). A critical review of supply chain management frameworks: Proposed framework, *Benchmarking: An International Journal*, *20*(2), 263-298.

South African Institute of Chartered Accountants (SAICA). (2013). *King III Report*. Retrieved from https://www.saica.co.za

South African Reserve Bank. (2013). *Registered banks*. Retrieved from http://www.resbank.co.za/RegulationAndSupervision/BankSupervision/Pages/SouthAfricanRegisteredBanksAndRepresentativeOffices.aspx.

Tan, J. (2001). *Forensic readiness*. Retrieved from http://www.atstake.com/research/reports/acrobat/atstake_forensic_readiness.pdf (Last accessed July 2010).

Valjarevic, A. & Venter, H. S. (2011). Towards a digital forensic readiness framework for public key infrastructure systems. *Proceedings of the 2011 Information Security for South Africa (ISSA) Conference*, Johannesburg, South Africa, 15-17 August 2011, ISBN 978-1-4577-1483-2.

Van Cleeff, A. (2008). Future consumer mobile phone security: A case study using the data-centric security model. *Information Security Technical Report*, *3*(3), 112-117. ISSN 1363-4127. doi:10.1016/j.istr.2008.10.003

Van Steenbergen, M., Bos, R., Brinkkemper, S., Van de Weerd, I. & Bekkers, W. (2010). The design of focus area maturity models. *Proceedings of the 5th international conference on Global Perspectives on Design Science Research*, pp. 317–332, Berlin and Heidelberg, Germany: Springer-Verlag. doi:10.1007/978-3-642-13335-0_2

Vinten, G. (1994). Participant observation: A model for organizational investigation? *Journal of Managerial Psychology*, *9*(2), 30-38.

Walliman, N. (2006). *Social research methods*. , London, UK: Sage.

Wespi, A., and Zunic, N. (2007). Elevating the discussion on security management: The data centric paradigm. *Proceedings of the 2007 2nd IEEE/IFIP International Workshop on Business-Driven IT Management (BDIM)*, pp. 84-93. In Munich. 21-25 May 2007.

Wheeler, E. (2010). *Digital forensic readiness checklist*. http://www.wareonearth.com/resources_forensics.html [6] (Accessed 12 August 2010).

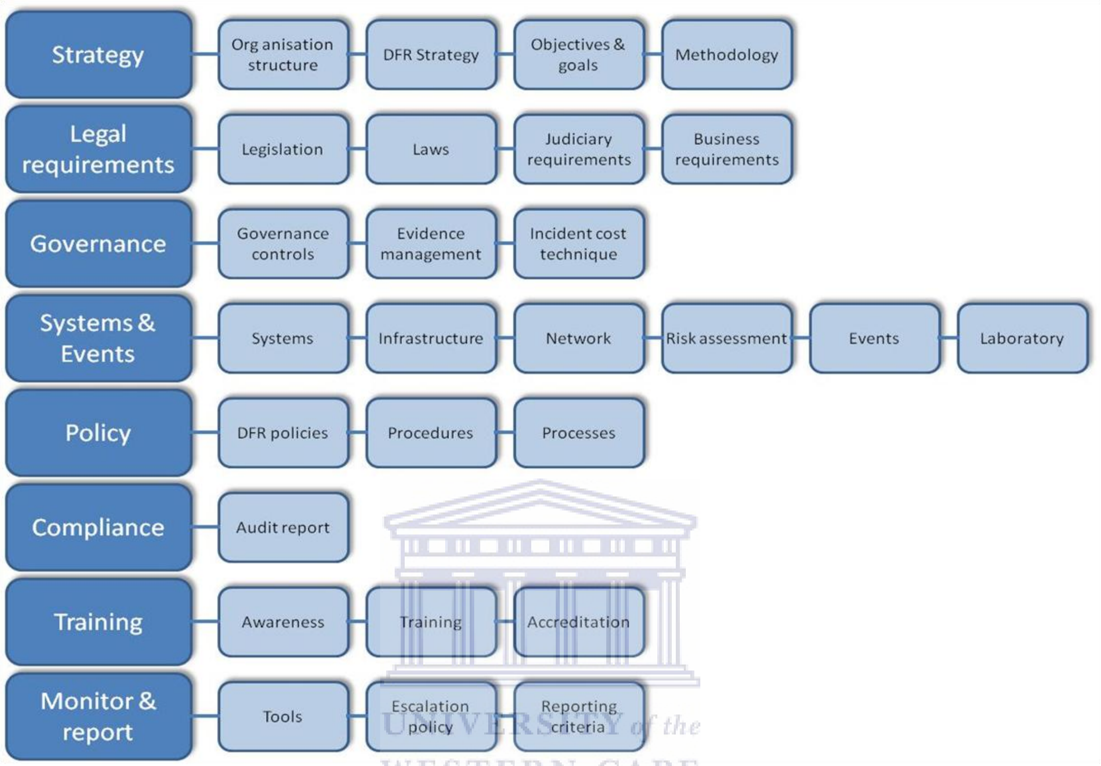
White, G. B. (2007). The community cyber security maturity model. Proceedings of the 40th Hawaii International Conference on System Sciences held in Hawaii, 3-6 January 2006.

Whyte, G. & Claims, I. (2012). The state of digital forensic readiness of financial services companies in South Africa. *Proceedings of the 3rd International Conference on Information Management and Evaluation (ICIME) 2012*, pp. 284-299. 16-17 April 2012, Ankara, Turkey.

Wilsdon, T & Slay, J (2005). Digital Forensics: Exploring Validation, Verification & Certification. *Proceedings of the First International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE'05)*, , pp. 48-55, held in Australia, 7-9 November 2005.

[6] The checklist was found on this website. However the website was since relocated to: http://ossie-group.org/ The checklist could not be found on this new website, but was requested via email at: info@ossie-group.org

APPENDIX 1: INTERVIEW QUESTIONS—Domains and sub-domains



Strategy	Org anisation structure	DFR Strategy	Objectives & goals	Methodology		
Legal requirements	Legislation	Laws	Judiciary requirements	Business requirements		
Governance	Governance controls	Evidence management	Incident cost technique			
Systems & Events	Systems	Infrastructure	Network	Risk assessment	Events	Laboratory
Policy	DFR policies	Procedures	Processes			
Compliance	Audit report					
Training	Awareness	Training	Accreditation			
Monitor & report	Tools	Escalation policy	Reporting criteria			

Question 1:

Find the above domains. How would you improve on them and can the sub-domains be further refined?

APPENDIX 2: INTERVIEW QUESTIONS—Model and Assessment Matrix

Check-box approach

Domains		Maturity levels				
Major domains	Sub domains	Level 1: Non-existent	Level 2: Basic	Level 3: Intermediate	Level 4: Advanced	Level 5: Full
		• No formalisation • As-and-when processes. • No documentation • No communication • No training • No regulation •	• Low formalisation • Repeatable processes. • Basic documentation • Low / informal communication • Informal training • Informally / ad-hocly regulated	• Standardised • Documented processes described in standards, procedures, tools, and methods. • Reviewed & accepted documentation • Communication to new staff on employment • Formal training • Formally regulated	• Endorsed by Exco. • Process improvement measurements in place. • Documents aligned with goals & objectives. • Communication to all staff annually. • Formal training & accreditation. • Principles are carried out, monitored and regularly improved.	• Endorsed by Exco. • Process improvement objectives for organization are established & effects of deployed process improvements are measured. • Changes to documents are incorporated & communicated. • Communication to all staff frequently. • Formal training & accreditation. • Legislations / laws / verdicts are studies and incorporated into processes, documents

Qualitative approach

Major domains	Sub-domains	Level 1: Non-existent	Level 2: Basic	Level 3: Intermediate	Level 4: Advanced	Level 5: Full
		No DFR strategy in place.	There is an undocumented tacit strategy that is communicated informally and ad-hocly.	Documented strategy endorsed by the executive management. It is communicated to IT / Forensic staff when joining the organisation.	Documented strategy endorsed by the executive management, highlighting the goals and objectives. It is communicated and made available to all staff at least once per annum. Staff are aware and know where to find the strategy.	Documented strategy endorsed by the executive management, highlighting the goals and objectives. It is made available and communicated to all staff regularly. Staff are aware and know where to find the strategy. Changes to the strategy and document are communicated to staff.

Question 2:

Find the above maturity model:

1.1 Which maturity assessment model would you prefer and why?

1.2 How can the maturity levels be further refined to illustrate an escalation from non-existence to full maturity?

APPENDIX 3—INTERVIEW TRANSCRIPTS

Interview 1 of 2 with XYZ Practitioners

Recording:	OMFIPR01
Site:	XYZ building, participant meeting room
Data collection method:	Formal interview
Data collection date:	15/08/2012
Data collector(s):	Ivan Claims
Transcriber:	Ivan Claims
Start time:	15:00 pm
End time:	15:08 pm
I:	Interviewer
R1:	Respondent one
R2:	Respondent two

[small talk]

-- *(Question 1: Find the above domains: how would you improve on them and can the sub domains be further refined?)* --

I: I emailed this [Pointing to the domain and sub domains on the projector] just to give you guys a heads up. I made this very simplistic. There is a lot we can discuss and honestly I-. I feel eager about this but do realise you guys have a lot of other work. I can honestly sit here and keep you guys busy for half a day, but I thought to keep it simple so I can also move ahead with my research. So these are the domains and sub domains [Pointing to the projector]. What I mean by domains and sub domains…when I went into literature … uhm…there are certain elements or certain things that stand out, that kinda need to be in place for a company that are considering DFR for example. One of those things was strategy, the other was legal requirements, then would be your governance, and then would be your policies, your compliance, and training, and monitoring and reporting. Now if I look at the first domain: strategy. Pieter Grobler , et al, they have published a lot of material concerning DFR , so one of the things they do mention is for example is your organisation structure, you need to have an overall DFR strategy, I think at corporate levels. And if you have other departments or units that also need to have a DFR strategy or strategic plan that is aligned with the overall strategy. Also there are objectives and goals that need to be factored in based on the overall DFR strategy. You also have to have some sort of methodology that needs to identify some sort of evidence collection need. In other words do you really need evidence, what kind of evidence, what kind of systems [Unclear]. So this is what I've done similarly with legal requirements. They have broken this down into legislation, laws, and judiciary requirements. Now judiciary requirement I can understand. What I understand from that would be…If there was a court case pending between an organisation and someone else…uhm…you know, because of forensic reasons. Whatever the verdict that might have come out of that, that kind of verdict needs to be studied and to see whether that is something that needed to be changed with in the organisation. One has to be cognisant of the verdicts that come out of those trials and assessments based on that. Of course we know there are certain legislations and certain laws, I don't know whether these per say could possibly be grouped together and just say…laws and regulations. Or would you want to put them separately because we might have different understandings of that. And of course you would have your business requirements, whatever business requirements you have one need to take…take…you know in cognisance the legal and judicial requirements based on that as well. Similarly with governance, you know we have to have governance controls, there has to be an evidence collection plan, and there has to be like an incident cost technique. Just to make an example…I mean you have to find out- First and foremost before you instigate an incident investigation find out whether it is feasible to go ahead or not. For example if it was like R500 and your investigation is going to cost more than that… really do you want to do that…but for you to be able to asses that you need to have a cost technique involved with that. Similarly with your systems and events. That's your systems, your infrastructure, your networks, your risk assessment, your events and your laboratory. I've never seen a laboratory before and I was hoping at some stage you could show me what is going on there, but typically these are the kind of things and organisation would have to go and identify and be aware of. What I've also heard…what I've seen is that actually do talk about some laboratories that have to be certified. I don't know if you guys have heard about that?. Uhm. Where you actually go for some certification because apparently that helps with…if you go and you submit your evidence in court…you know that kind of gives you a heads up.

--5 minutes into the interview --

R2: That helps if you're a private company, and you need to show to clients that you have a certain level of expertise and equipment. You say okay I'm ISO 9000 compliant. Cause the client also has an obligation from their side. You know…we will only do business with vendors who are certified, whatever, whatever.

I: Ok

R2: Internally, I don’t think the law requires that the lab itself be certified.

R1: I think certifications are more appropriate to training aspects, so individuals could be certified regardless of your tools and environment. If an individual has a certain level of certification that says yes maybe I don’t have [Unclear] I know enough to make sure the evidence is not contaminated. So you can mitigate. Cause some of those certification criteria just doesn’t make sense in our environment.

I: When you say our environment, do you mean South African environment…or?

R1: Corporate environment.

R2: Corporate environment

R1: I can understand that Scotland Yard…whatever might, but for 90 cases out of a 100 that just turns into a disciplinary, I don’t see why every time I must rebuild my system…clean and all that. It just doesn’t make sense.

I: Yes

R1: The software wouldn’t really allow cross contamination of evidence and-. In a disciplinary that discussion goes away very quickly.

I: Ok

R1: It’s not like a major court case, where-. Yes I would rather-

I: uhuh

R2 Maybe if I can start commenting.

I: Ok

R2: This whole- well not completely yet. Alot of what you put there [Pointing to the domains and sub domain on the projector] the way we work…is not necessary the way all companies work, but digital forensics is a sub component of a forensic perspective. So to say you have a default strategy is absolutely meaningless in our environment.

I: Ok

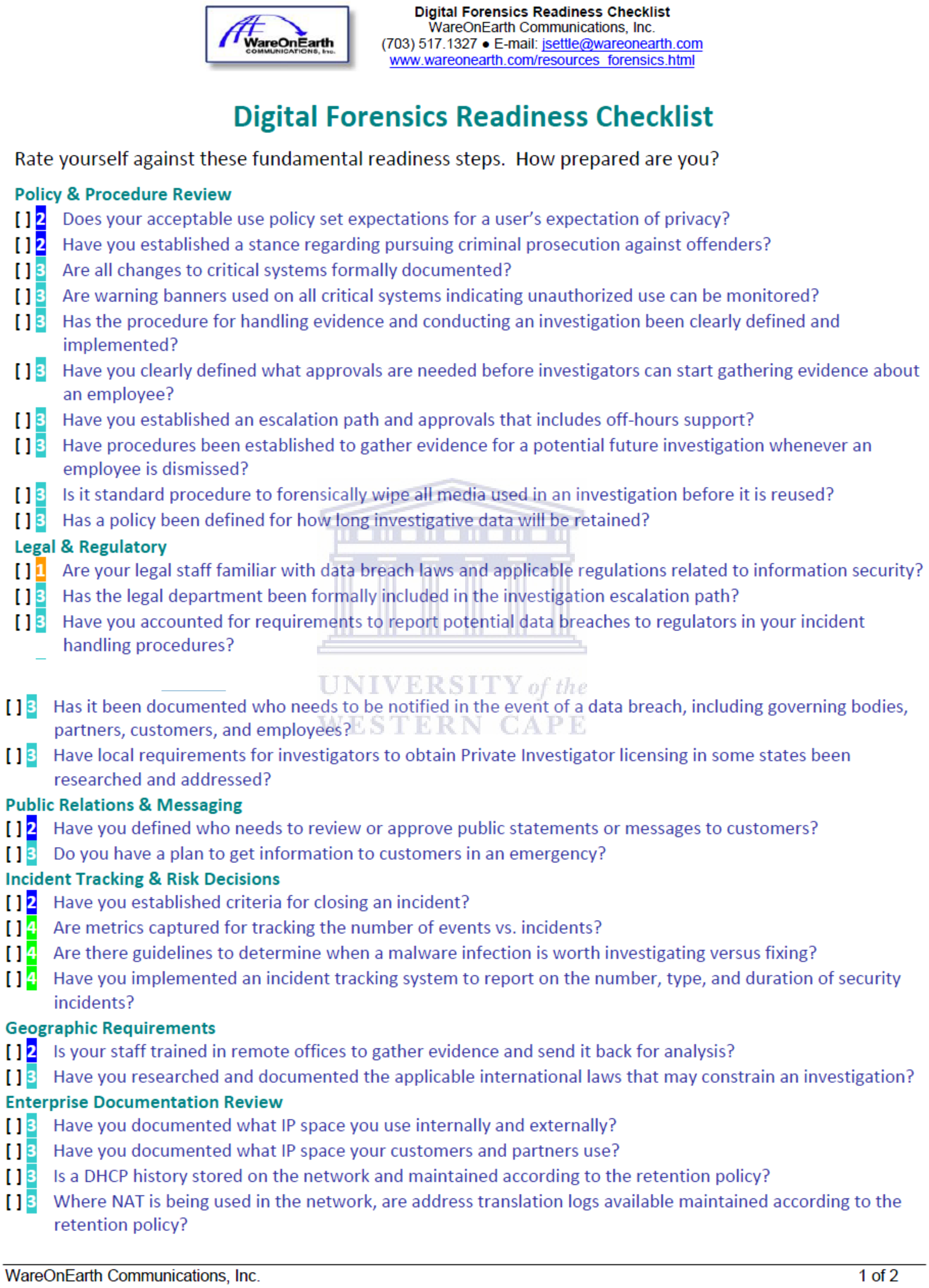
R2: We’ve got a forensic need and similar to handwriting experts, or lie detection, what’s the word, but these kinds of functions. Digital forensics is actually just another specialist kind of tool that the forensic investigator makes use of.

I: Ok

[Interview 1 was permanently disrupted by the device. See interview 2 for the continuation of the conversation]

-- End of the interview which lasted 7:37 minutes --

APPENDIX 4—DIGITAL FORENSIC READINESS CHECKLIST



Digital Forensics Readiness Checklist
WareOnEarth Communications, Inc.
(703) 517.1327 • E-mail: jsettle@wareonearth.com
www.wareonearth.com/resources_forensics.html

Digital Forensics Readiness Checklist

Rate yourself against these fundamental readiness steps. How prepared are you?

Policy & Procedure Review

[ ] 2 Does your acceptable use policy set expectations for a user's expectation of privacy?
[ ] 2 Have you established a stance regarding pursuing criminal prosecution against offenders?
[ ] 3 Are all changes to critical systems formally documented?
[ ] 3 Are warning banners used on all critical systems indicating unauthorized use can be monitored?
[ ] 3 Has the procedure for handling evidence and conducting an investigation been clearly defined and implemented?
[ ] 3 Have you clearly defined what approvals are needed before investigators can start gathering evidence about an employee?
[ ] 3 Have you established an escalation path and approvals that includes off-hours support?
[ ] 3 Have procedures been established to gather evidence for a potential future investigation whenever an employee is dismissed?
[ ] 3 Is it standard procedure to forensically wipe all media used in an investigation before it is reused?
[ ] 3 Has a policy been defined for how long investigative data will be retained?

Legal & Regulatory

[ ] 1 Are your legal staff familiar with data breach laws and applicable regulations related to information security?
[ ] 3 Has the legal department been formally included in the investigation escalation path?
[ ] 3 Have you accounted for requirements to report potential data breaches to regulators in your incident handling procedures?

[ ] 3 Has it been documented who needs to be notified in the event of a data breach, including governing bodies, partners, customers, and employees?
[ ] 3 Have local requirements for investigators to obtain Private Investigator licensing in some states been researched and addressed?

Public Relations & Messaging

[ ] 2 Have you defined who needs to review or approve public statements or messages to customers?
[ ] 3 Do you have a plan to get information to customers in an emergency?

Incident Tracking & Risk Decisions

[ ] 2 Have you established criteria for closing an incident?
[ ] 4 Are metrics captured for tracking the number of events vs. incidents?
[ ] 4 Are there guidelines to determine when a malware infection is worth investigating versus fixing?
[ ] 4 Have you implemented an incident tracking system to report on the number, type, and duration of security incidents?

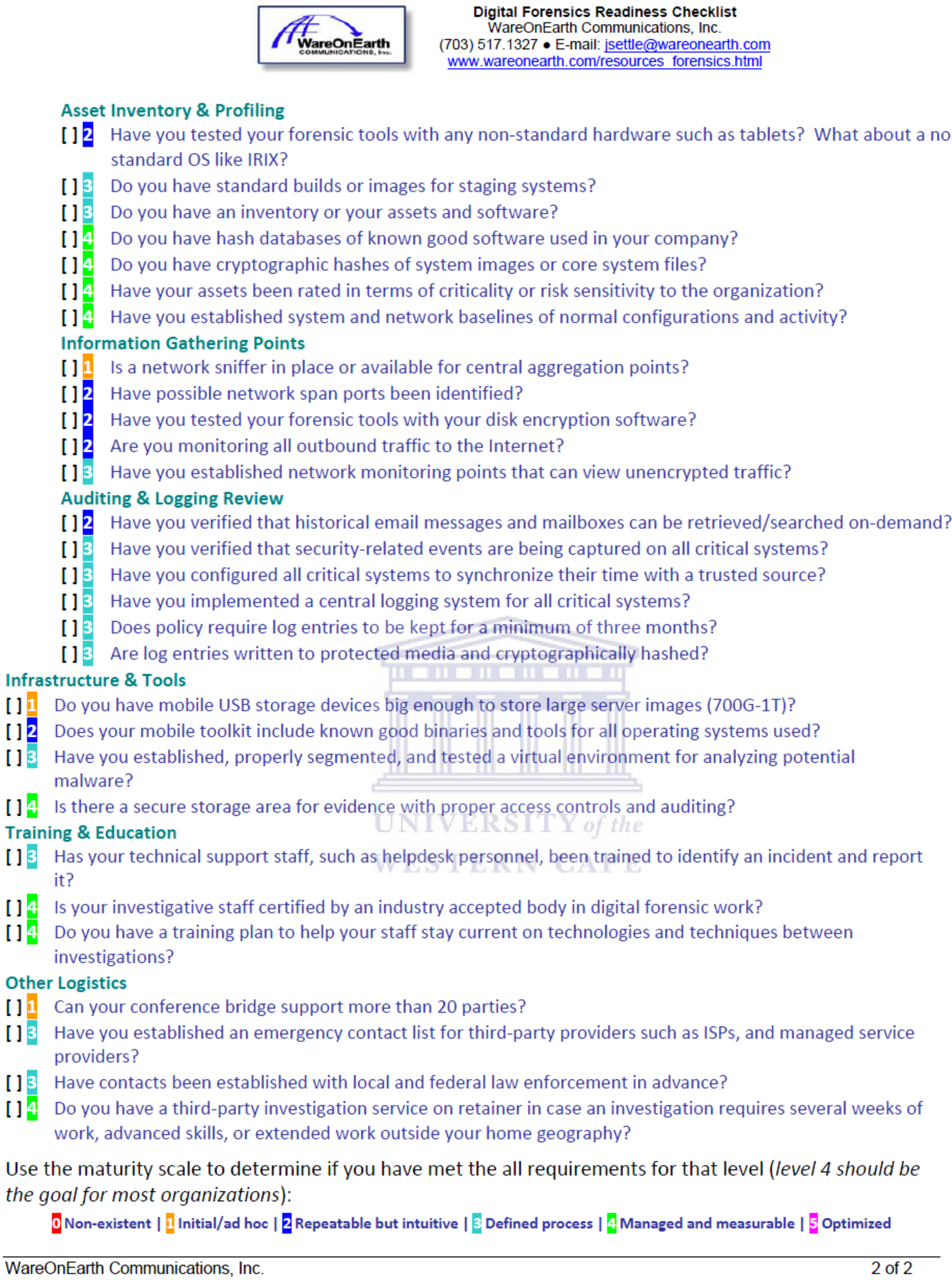
Geographic Requirements

[ ] 2 Is your staff trained in remote offices to gather evidence and send it back for analysis?
[ ] 3 Have you researched and documented the applicable international laws that may constrain an investigation?

Enterprise Documentation Review

[ ] 3 Have you documented what IP space you use internally and externally?
[ ] 3 Have you documented what IP space your customers and partners use?
[ ] 3 Is a DHCP history stored on the network and maintained according to the retention policy?
[ ] 3 Where NAT is being used in the network, are address translation logs available maintained according to the retention policy?

WareOnEarth Communications, Inc. 1 of 2



Digital Forensics Readiness Checklist
WareOnEarth Communications, Inc.
(703) 517.1327 • E-mail: jsettle@wareonearth.com
www.wareonearth.com/resources_forensics.html

Asset Inventory & Profiling

[ ] 2 Have you tested your forensic tools with any non-standard hardware such as tablets? What about a non-standard OS like IRIX?
[ ] 3 Do you have standard builds or images for staging systems?
[ ] 3 Do you have an inventory or your assets and software?
[ ] 4 Do you have hash databases of known good software used in your company?
[ ] 4 Do you have cryptographic hashes of system images or core system files?
[ ] 4 Have your assets been rated in terms of criticality or risk sensitivity to the organization?
[ ] 4 Have you established system and network baselines of normal configurations and activity?

Information Gathering Points

[ ] 1 Is a network sniffer in place or available for central aggregation points?
[ ] 2 Have possible network span ports been identified?
[ ] 2 Have you tested your forensic tools with your disk encryption software?
[ ] 2 Are you monitoring all outbound traffic to the Internet?
[ ] 3 Have you established network monitoring points that can view unencrypted traffic?

Auditing & Logging Review

[ ] 2 Have you verified that historical email messages and mailboxes can be retrieved/searched on-demand?
[ ] 3 Have you verified that security-related events are being captured on all critical systems?
[ ] 3 Have you configured all critical systems to synchronize their time with a trusted source?
[ ] 3 Have you implemented a central logging system for all critical systems?
[ ] 3 Does policy require log entries to be kept for a minimum of three months?
[ ] 3 Are log entries written to protected media and cryptographically hashed?

Infrastructure & Tools

[ ] 1 Do you have mobile USB storage devices big enough to store large server images (700G-1T)?
[ ] 2 Does your mobile toolkit include known good binaries and tools for all operating systems used?
[ ] 3 Have you established, properly segmented, and tested a virtual environment for analyzing potential malware?
[ ] 4 Is there a secure storage area for evidence with proper access controls and auditing?

Training & Education

[ ] 3 Has your technical support staff, such as helpdesk personnel, been trained to identify an incident and report it?
[ ] 4 Is your investigative staff certified by an industry accepted body in digital forensic work?
[ ] 4 Do you have a training plan to help your staff stay current on technologies and techniques between investigations?

Other Logistics

[ ] 1 Can your conference bridge support more than 20 parties?
[ ] 3 Have you established an emergency contact list for third-party providers such as ISPs, and managed service providers?
[ ] 3 Have contacts been established with local and federal law enforcement in advance?
[ ] 4 Do you have a third-party investigation service on retainer in case an investigation requires several weeks of work, advanced skills, or extended work outside your home geography?

Use the maturity scale to determine if you have met the all requirements for that level (*level 4 should be the goal for most organizations*):

0 Non-existent | 1 Initial/ad hoc | 2 Repeatable but intuitive | 3 Defined process | 4 Managed and measurable | 5 Optimized

WareOnEarth Communications, Inc. 2 of 2