Forensic Science International: Digital Investigation 40 (2022) 301348

Contents lists available at ScienceDirect

Forensic Science International: Digital Investigation

journal homepage: www.elsevier.com/locate/fsidi

An extended digital forensic readiness and maturity model

Felix Bankole, Prof [a, *], Ayankunle Taiwo [b], Ivan Claims [c]

[a] Artificial Intelligence Cluster, School of Computing, University of South Africa, South Africa
[b] Computer Information Technology Department, Schreiner University, Kerrville, Texas, USA
[c] University of the Western Cape, South Africa

ARTICLE INFO

Article history:
Received 27 August 2021
Received in revised form
6 January 2022
Accepted 10 January 2022
Available online 28 January 2022

Keywords:
Digital forensic readiness
Digital forensic commonalities framework
Digital forensic maturity model
Climate change
COVID19 pandemic and beyond
Computing
Analytics and decision models
IS Global

ABSTRACT

Digital forensics readiness (DFR) is an important part of the growing forensic domain. Research on DFR has been given little attention, while available DFR models have focused on theoretical investigations with inadequate input from practicing information security experts in the industry. Using feedback from practicing forensic experts in the industry and academia, this research investigates the structure required to implement and manage digital forensic readiness (DFR) within an enterprise. The research extended the DFR Commonalities framework (DFRCF) and utilised the structure to design a digital forensic maturity assessment model (DFMM) that will enable organisations to assess their forensic readiness and security incident responses. A combination of qualitative and research design approaches was utilised to perform a comparative analysis of various DFR frameworks. A top-down design approach was utilised in developing the DFMM model which was validated with forensic practitioners and academics through semi-structured interviews. The structure extracted from DFR frameworks was practical since most participants agreed with the structure of the extended DFRCF and the matrix of the maturity model.

Overall, key changes were introduced to enhance both the extended DFRCF and the DFMM. The study was limited to participants who have a forensic footprint and are knowledgeable about DFR. This paper thereby provides practitioners, academics and organisations with access to a non-propriety DFMM maturity model.

1. Introduction

The importance of digital forensics and the use of digital evidence in the forensic domain continues to grow (Pollitt et al., 2018), cyber criminals and security specialist are both making extensive use of technology (Rege and Mbah, 2018). Thus, the importance of cybersecurity and the corresponding digital forensics cannot be overemphasised. Therefore, it is important to secure corporate enterprises against cyber-attacks as well as learning from digital evidences left after intrusion, and to be digital forensically ready for any form of cyber/digital incident. Within the digital forensic domain, there is a plethora of research work on digital forensic investigation models (Ariffin and Ahmad, 2021). However, the term "digital forensics readiness" have been given little or inadequate attention.

Digital Forensic Readiness (DFR) is an anticipatory approach that resides within the digital forensics' domain and is used for digital evidences (Tan, 2001; Kebande and Venter, 2019). In order to implement or manage Forensic readiness in an organization, it is imperative to understand the structures required before investing in the required resources. It is necessary for the organisation to have an assessment tool to measure the level of DFR maturity, as failure to do so exposes the organisation to cyber incidents (e.g., economic crimes), since the weaknesses and the opportunities to strengthen the preparedness against cyber incidents remains undiscovered. Furthermore, an organisation's failure to assess its DFR preparedness highlights the possible mismanagement of its DFR programme. Although aimed at project management, this view is supported by Ramirez, (2002). It should be remembered that the King III report also recommends that all controls within an organisation must be assessed and the results documented (Grobler et al., 2010a). The implication of this is that the DFR programme, aimed at controlling and mitigating cyber incidents, needs to be assessed.

Despite existing protections, data breach still occurs (Posey et al., 2017), but details on digital forensics security incidents

* Corresponding author.
E-mail addresses: bankofo@unisa.ac.za (F. Bankole), ataiwo@schreiner.edu (A. Taiwo).

https://doi.org/10.1016/j.fsidi.2022.301348
2666-2817/

from financial organizations are rarely published. Therefore, many studies examine experimental, simulated or hypothetical incidents for digital forensics security incidents (Dykstra and Sherman, 2011; Teing et al. 2016). However, Weiss & Miller (2015) have investigated a financial data breach that occurred in Target, a US based supply chain organization. Cyber criminals breached financial data that was reported in 2013 to have cost Target about $248 million (as the data breach was reported in 2013). The Target financial breach report was made public as a result of US legislative action in the 114th Congress payment systems development. Other organizations that have suffered major digital forensics security incidents such as data breaches includes; Sony, Adobe, Home Depot and JPMorgan Chase where payment card information was obtained by hackers. Targets and other organizations had to hire outsiders to conduct digital forensics security incident investigations (Weiss & Miller,2015). In South Africa, major data breaches have occurred that suggest that much South African information has been exposed to cybercriminals (Kempen, 2017). Thus, DFR becomes critical for most financial organizations and their business clients.

In accordance with the identified problem of growing reports of cyber-attacks on financial institutions compromising large volumes of financial data (Arde, 2012; Niekerk,2017), the main established research question is to investigate DFR structures (domains) that are needed by financial services businesses, and how to develop a maturity assessment model using these domains that use DFR to anticipate security incidents that might occur as a result of a pandemic such as COVID19, and other unexpected disasters and beyond. Therefore, the objective of this research is to develop a Digital Forensic (DFMM) Maturity Model. The main contributions of this paper are: (1) Extending the Digital Forensics Readiness Commonalities Framework (DFRCF) of Whyte and Claims (2012) with Digital Forensics Management Framework (DFMF) of Grobler et al., (2010a). (2) Proposing a non-proprietary new Digital Forensic maturity model, and validated with forensic practitioners and academics. To achieve this, a combination of research and qualitative interpretive approaches grounded on thematic fundamentals were used.

2. Literature review

2.1. Digital forensic readiness (DFR- models)

Digital Forensic Readiness (DFR) is an anticipatory approach that resides within the digital forensics domain and seeks to maximise an organisation's ability to collect digital evidence while minimising the cost of such an operation (Tan, 2001; Kebande & Venter,2019). The goal of any threat intelligence gathering is to gain rich evidence that can aid decision making, thus the maturity, the skills, and the information sources of a security team define their capability to produce accurate and urgent actionable threat information (Rid and Buchanan, 2015; Johnson et al., 2016). Benefits of threat intelligence include improved efficiency and effectiveness in security operations in terms of detective and preventive capabilities (Mavroeidis and Bromander, 2017). However, information security scientists and digital forensic incident experts need the right skills to recognize attacks before performing defence efforts. The development of adequate controls requires a thorough threat analysis, but most of the time small, medium sized and even large businesses have inadequate capabilities, due to lack of skilled personnel and budget constraints (Mavroeidis and Bromander, 2017). This has resulted in proposals for frameworks for digital forensic intelligence, of which a notable example is that proposed by Quick and Choo (2018).

Most existing models on security are reactive rather than proactive (Le and Hoang (2017), and do not provide an adequate guide in for preventing forensic and security incidents. In a previous study, Spruit and Röling (2014) have proposed an Information Security maturity model that features Organization, Technical, Organization & Technical and Support categories. Spruit & Röling further suggest a model alignment with business in non-IT areas. Organisations spend vast resources in their endeavour to align their maturity assessment models with the DFR goals and objectives. To alleviate this, a few studies in literature have proffered standards and frameworks geared towards efficient digital forensic investigations and readiness as shown in Marshall (2011) and Sachowski (2016). For example, in South Africa, large volumes of both financial and personal identifiable data breaches have been reported by (Niekerk, 2017). Thereby revealing inadequate digital forensic readiness and preparedness for cybersecurity incidents.

The overall alignment model is an example of a model that seeks to align Information Technology (IT) with business strategy (Henderson and Venkatraman, 1993). A similar model, called the strategic alignment model has been presented by Luftman et al. (1993). It is therefore reasonable to conclude that misalignment of entities has undesired effects on a business. This results in many resources being used, and large efforts being made by organisations to align these activities after implementation rather than before. It would therefore be preferable to develop a DFR security framework that is aligned with the objectives and goals of DFR and is compliant with the current pandemic and beyond (Ågerfalk, Conboy & Myers, 2020). This framework would align with the strategies of climate change adaptation and sustainability.

2.1.1. Digital forensics readiness commonalities framework (DFRCF)

Drawing upon the previous works of Tan (2001) and Rowlingson (2004), Whyte and Claims, 2012) have developed DFRCF using a ten (10) step approach. The DFRCF is a framework that specifies forensic readiness by considering the interconnectedness of domains and subdomains. DFRCF describes seven (7) domains that make up the structure of the framework. Fig. 1 illustrates the scope of the framework. The framework is presented in the form of a wheel with the *Legal Involvement* domain as the axis. The sub domains are hidden within each domain.

2.1.1.1. Strategy. The rationale behind this domain is to ensure that an organisation has; a DFR strategy aligned to the organisation's

Fig. 1. DFR Commonalities framework (Whyte and Claims, 2012).

goals, an organisational structure that highlights the reporting lines of the forensic unit and has a technique constructed to evaluate the evidence collection requirements (Grobler et al., 2010a; Grobler et al., 2010b). The strategy domain is included in this study to foster outputs such as; organisation structure depicting the forensic unit and responsibilities; DFR strategy that illustrates the objectives and goals. It could be argued that the purpose of this domain is to promote an enterprise-wide adoption of proactive digital forensics in an organisation. The versatility of the corporate DF strategy will in-variably drive the governance of the detailed DF policies (Whyte and Claims, 2012).

2.1.1.2. 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 establishment of a laboratory equipped with technologies and DF tools to do proper investigations is crucial within the DF realm (Grobler et al., 2010). Wilsdon and Slay (2005) suggest that the laboratory should strive towards ISO17025 certification as this validates that a laboratory is proficient at constructing technically valid data and results. The following are all the possible outputs that can be produced when completing all the sub-domain activities within this domain: 1. identification and classification of source systems, 2. identification of business events and risk assessment. 3. List of systems and infrastructure requirements and 4. Plan to acquire laboratory competence and accreditation. Implementation of DF systems and events further presents a need for policy requirements (Whyte and Claims, 2012).

2.1.1.3. Policy. This domain ensures that underlying policies and procedures are implemented according to agreed standards, as identified within the Governance domain. Each organisation should assess its policy requirements. Policy requirements are possible outputs that can be produced when completing all the sub domain activities within this domain. This domain satisfies the DFR benefit of evidence gathering and preparing data for investigation leads. The successful design of the policy domain provides a foundation for the consideration of a user's compliance with the stated DF policies (Whyte and Claims, 2012).

2.1.1.4. Compliance. This domain is concerned with user conformance to DFR policies, legislation and procedures (Bonanzi et al., 2010). Audit reports that measure conformance to governance requirements are the possible outputs that can be produced when completing all the activities within this domain. This domain fosters the DFR benefit of preventing anti-forensic activities and the use of DF tools in organizations. Subsequently the outputs from audit reports will advise on areas where user training is needed (Whyte and Claims, 2012).

2.1.1.5. 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). Laboratory certification must also be part of the training objective (Wilsdon and Slay, 2005). The following are possible outputs that can be produced when completing the sub domain activities within this domain: 1. Awareness campaigns. 2. Training strategy with accredited training programmes. This domain fosters the DFR benefit of allowing an investigation to proceed at a cost in proportion to the incident (Whyte and Claims, 2012).

2.1.1.6. Monitor and report. There is need for constant monitoring after training to understand the return on training investments from which users benefit**.** This domain ensures that the organisation compiles DF Incident report requirements (such as the report format, and so forth) and have an incident escalation policy. A cost/benefit analysis must be done before an investigation is commenced in order 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: 1. Reporting criteria (report format, report requirements, and so forth) and incident escalation policy. 2. Cost/benefit analysis and a needs analysis for Monitoring tools. 3. How IDS triggers should function and respond. 4. Guidelines for interaction between concerned parties. This domain fosters the DFR benefit of evidence gathering, data preparing and cost investigating in proportion to the incident (Whyte and Claims, 2012).

2.1.1.7. Legal requirements. 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. Legal requirements must inform all outcomes within the framework (Rowlingson, 2004). It is thus reasonable to state that the use of this domain in a maturity model when managed to perform all the activities within the domains, will ensure that all the goals and objectives of DFR are met. This also means that an assessment model that is utilising all the components of DFRCF, strives to satisfy the goals and objectives of DFR and security incidents. Furthermore, the resulting maturity model will provide an opportunity to contribute to the enhancement of DFR benefits and security incidents. Therefore, this research includes this domain to promote an enterprise-wide adoption of proactive digital forensics (Whyte and Claims, 2012).

2.1.2. Digital forensics management framework (DFMF)

Grobler et al. (2010a) have presented the DFMF which is a layered model that helps to manage forensic readiness capability in an organization. DFMF presents six domains and various sub-domains that constitute the structure of the framework. Fig. 2 illustrates the scope of the framework. The framework is displayed as a flat, layered box, which makes the underlying sub-domains visible.

2.1.2.1. Governance. This is a domain within DFMF that advocates the establishment of an overall DF policy. This domain is critical and is adopted for use in this study because it has exhaustive DF sub-domains including guidelines to ensure uniformity across the enterprise. Governing bodies should ensure that the policies and policy frameworks are implemented according to agreed standards (Grobler et al., 2010a) and that there should be a clear and explicit separation of responsibilities. Investigations should not be approved by the same group that is performing them.

The concluding comparative analysis that has been performed between the digital forensic readiness commonalities framework (DFRCF) and the digital forensics management framework (DFMF) has resulted in the extension of the DFRCF. Table 1 gives a summary of the comparative analysis of the digital forensics' models carried out by Ab Rahman and Choo (2015).

2.2. Shortfall in existing DFR frameworks

Reith et al. (2002) have examined digital forensic models and have found that an unavailability of Digital Forensic standardization has resulted in many works showing procedure and frameworks that are too technology specific, making it difficult to generalize them to digital forensics studies. With little emphasis on policy domains or practitioner input, an integrated conceptual digital

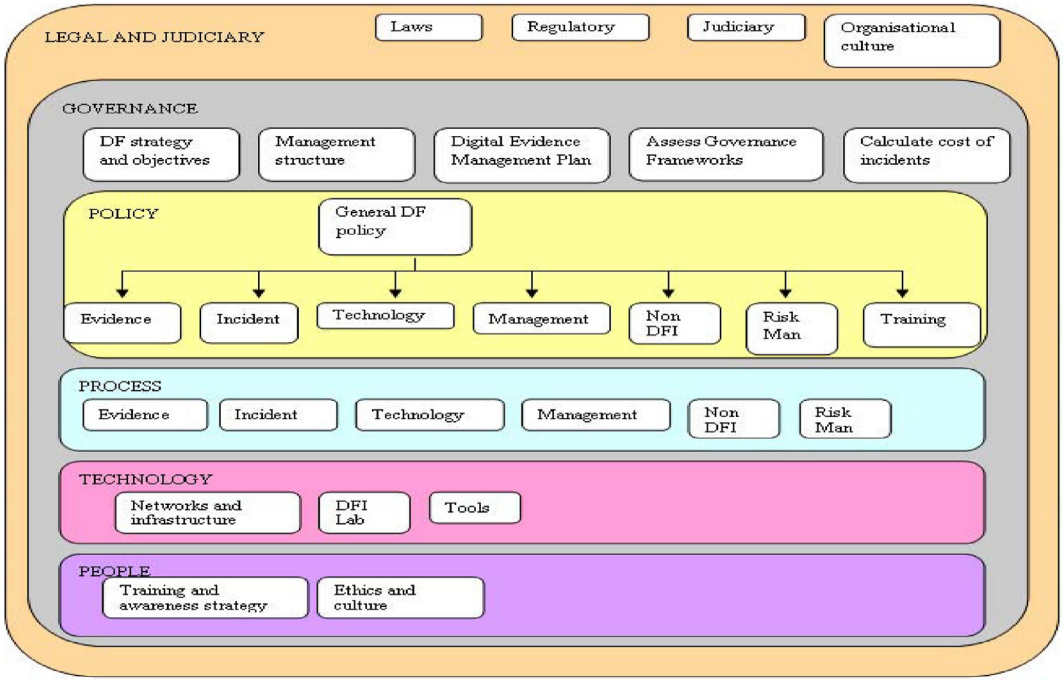

Fig. 2. DFMF and its elements (Source: Grobler et al., 2010a).

forensic framework has been proposed by Martini and Choo (2012) with an effort to identify differences in secure storage of forensic data and data stored in the cloud for forensic purposes. Verma, Govindaraj and Gupta (2018) have proposed an application Digital Forensics Framework with secure a logging mechanism that uses case information, profile data and expert's knowledge of the case for automation. However, Verma et al. (2018) have focused on machine learning application development using case data with little or no evidence of policy implementation. Baror, Venter and Adeyemi (2020) have proposed a DFR framework that employs the use of natural language processing techniques to develop a process for cybercrime detection in a real-time like version in a cloud environment. The synthesis of medical devices and health care systems known as medical cyber-physical systems (MCPS) have created a new attack vector for malicious actors in the network whereby a breach by financially and criminally motivated actors can impact patient data and systems failure. For instance, some pieces of medical apparatus are equipped with embedded software and integrated interfaces which generate vast amounts of data that could be compromised by an intruder (Grispo, Glissson and Choo, 2017). Because of these technology specific applications, this paper attempts to produce a framework applicable to a variety of technologies and industries.

2.3. Digital forensic readiness and digital security incidents

According to previous works on DFR and digital forensic investigations, studies have presented theoretical models with little input from forensic practitioners. For instance, Alenezi, Hussein, Walter and Wills (2017a) have investigated the digital forensic readiness in cloud computing, and propose a framework depicting important organizational, technical and legal factors that influence digital forensic readiness of an organization. Furthermore, Alenezi et al. have emphasized the need for stakeholders such as forensic experts and IT practitioners to validate models and frameworks. Alenezi et al. (2017b) have examined the impact of cloud forensic readiness on security and identify an overlap of DFR and security as a converging area with a suggestion that further studies are needed. Park et al. (2018) investigating the DFR design cloud computing-based environment, have designed a DFR model to deduce work areas that need close attention to avoid a security incident, have collected IT practitioner's data and have found that user information and usage information are most critical. However, survey data validity verification has not been reported. Chernyshev, Zeadally & Baig (2019) have closely examined the DFR of health institutions after health care data breaches and have found privilege misuse is a critical factor that causes the breach and propose a conceptual architecture for forensic audit loggings to support digital forensic investigations. As discussed above, many previous studies on DFR do not consider the input of IT practitioners in their studies. In this paper, we consider experts opinion in the development of the maturity model.

2.4. Industry statistics for cyber-incidents and threats

Niekerk (2017) investigated cyber-incidents, and discover prevalent incidents occur through malicious hackers trying to break into the computer network. This threat brings about data exposure to malicious individuals. Forty six percent (46%) of cyber incidents have occurred in private and non-governmental organizations. This statistic is considered consistent with global reports on cyber incidents. In a related study on cyber-crimes, Baror and Venter (2019) have suggested the need for digital forensic readiness and found that non-technical induced cybercrime techniques are used for 61% of public cloud cybercrime incidents. These incidents have been attributed to an inadequacy of traditional digital forensic frameworks that can be used in tackling cybercrime in the public cloud.

Alenezi et al. (2017a) have investigated the impact of Forensic Readiness on cloud-security and suggest that the volume of cyber threats is on the increase with few studies on cloud forensic readiness. Alenezi et al., (2017b) have provided no digital forensic readiness framework but postulate the need to investigate digital forensic readiness due to increases in the number of cyber

Table 1
Comparative study of digital forensic models (source: Ab Rahman and Choo, 2015).

Model Components	Cohen	Pilli et al. (2010)	Agarwal et al. (2011)	Martini and Choo (2012)	Wu et al. (2013)	Valjarevic and Venter (2011)	Kohn et al. (2006)	Quick and Choo (2018)	Quick and Choo (2018)
Phases		Preparation & Authorisation	Preparation		Identification & Preparation	Planning Processes Group	Preparation	Commence, Prepare & Response	Commence, Prepare & Response
	Identification	Detection of Incident/Crime	Securing the Scene Survey & Recognition	Evidence Secure Identification & Preservation	Identifying Data Sources		Incident Response		
		Incident Response	Documenting the Scene Communication Shielding		Prioritising, Preservation & Collection		Incident Response		
	Collection	Collection	Evidence Collection	Collection		Assessment Processes Group	Physical Digital Forensic Investigation	Preservation Analysis	Collection
	Transportation Storage	Preservation Examination & Analysis	Preservation Examination & Analysis	Examination & Analysis	Examination & Analysis				Examination & Analysis
	Examination & Traces	Investigation							
	Presentation	Presentation	Presentation	Reporting & Presentation	Reporting & Presentation	Implementation Processes Group	Presentation & Documentation	Presenting feedback Complete or Future tasks identified (second iteration)	
	Destruction	Review	Result & Review		Review Results				
Forensic Readiness	No	Yes	Yes	No	Yes	Yes	Yes	Yes	
Domain	Generic	Network Forensic	Generic	Cloud Computing	Critical Infrastructure	Generic	Generic	Cloud Storage	Cloud Computing

incidents. In a study on digital forensic readiness in organizations, Karie and Karume (2017) suggest inadequate guidance (training) and adherence to policy as two of the challenges that affect many organizations in making their organizations digital forensic ready. In a related study investigating the digital forensic readiness of an automated substation in the Power Sector. In similar study, Iqbal et al. (2018) have found that despite that fact that the organization maintains a critical infrastructure, it does not have the ability or framework to detect cyber-attacks on causing signal loss or data spoofing.

2.5. Benefits of implementing digital forensic readiness

According to Rowlingson (2004), the goal of implementing DFR is to collect digital evidence targeting the potential crimes and disputes that may adversely impact an organisation. The successful implementation of DFR helps to prevent anti-forensic activities, enhances performance of digital forensic tools, fosters effective forensic controls, provides data for investigation leads, gathers evidence and promotes the integrity of evidence for legal actions (Bradford et al., 2004; Grobler et al., 2010a, 2010b). Successful implementation of DFR helps organizations to limit the number of incidents that will occur by selecting and implementing a set of controls (Cichonski et al., 2012), maximises the potential to use comprehensive digital evidence (Grobler et al., 2010a; Grobler et al., 2010b) and minimise the cost of forensics during response in proportion to the incident (Pangalos et al., 2010).

2.6. Maturity models for digital forensic readiness and security incidents assessment

As mentioned in the introduction section of this research, organisations integrate and assess DFR in 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). 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".

Secondly, forensics is applied to less than 30% of business security incidents (Pangalos et al., 2010a). 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 assessments 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 et al., 2010b). It is thus conceivable that an information security assessment will not have a DFR focus. It is also reasonable to argue that Information Security focused assessment models will not emphasise the need to exclusively achieve the goals of a DFR framework.

Thus, due to the above-mentioned shortcomings with attempting to utilise information security assessment to assess DFR and, due to the inadequacy of existing DFR and security incident(s) maturity assessment models, this research develops a DFMM maturity model based on the structure of the extended DFRCF framework.

3. Research design and methodology

We adapted the maturity assessment models design science approach of (Mettler, 2011) and the IS security policy design theory guidelines proposed by Siponen and Iivari (2006). The five steps of the design science methodology process and the corresponding output are shown in Table 7. The methodology used in this study is qualitative approach whereby participants were interviewed and the equivalent input were analysed using thematic analysis.

Consequently, nomothetic design science process was employed (Baskerville et al., 2015), Nomothetic design suggests generalizable design theories, with the employment of generic design principles that can be applied to specific classes of challenges (Markus et al., 2002; Kang and Hovav, 2020). Explanatory design methodology in applied research can be used to validate Nomolithic design (Kang and Hovav, 2020). Previous studies such as Baskerville et al. (2015) have detailed similar methodology to the work of Mettler (2011) on research design, while Njenga and Brown (2012), Cram and Proudfoot & D'Arcy (2017) discuss work similar to Siponen and Iivari (2006). The following research questions are asked:

1. What DFR structure (elements or domains) is needed by financial services businesses?
2. How can such a structure contribute to the design of a maturity assessment model?

Suggested steps in the research design of maturity assessment models (Mettler, 2011) are listed below:

Step1 Identify the need and specify the problem domain: *Misalignment of entities that should be aligned has undesired effects on a business*.
Step2 Define the scope of the model application and use
Step3 Design model: Identify the operationalization measures (*See Fig. 3 and Theoretical framework section*)
Step4 Evaluate design (*See section on Discussion of Findings*)
Step5 Reflect evolution: Synthesis of design and continuous learning (See Table 7)

The DFRCF was combined with the domains of DFMF to answer the research questions above, and to produce an extended DFRCF. Fig. 3 shows a graphical depiction of the extended DFRCF, i.e., before forensic expert participant input. The extended DFRCF consists of major domains and their respective sub domains that must all be assessed by the DFR maturity model.

The extended DFRCF model is a more comprehensive and functionally oriented model when compared with, for example, the approaches employed in enhancing security incident response follow-up efforts with lightweight agile retrospectives by Grispos et al. (2017). argue that many security incident response approaches incorporate a feedback or follow-up phase. However, these approaches provide little practical information about the tools and/or techniques that could be employed to extract lessons learned from security incident investigations. In the same manner, they explain that most organizations focus on improving technical controls and do not reassess the effectiveness of internal policies and procedures that have a great impact by contributing to the incident or obstructing investigative efforts. Additionally, there are limited tools or technical supports for an organization to evaluate whether or not enhancements have been implemented, when it extracts lessons learned from security incident investigations.

Hence, the research of Grispos et al. (2017) has examined the impact of integrating lightweight agile retrospectives into a security incident response environment. This approach presents lightweight retrospectives as a means of enhancing security incident response follow-up efforts and provides an empirical evaluation/validation of this lightweight approach in a Fortune 500 financial organization security incident response team. This shows that it is an acceptable solution for driving the development of lessons

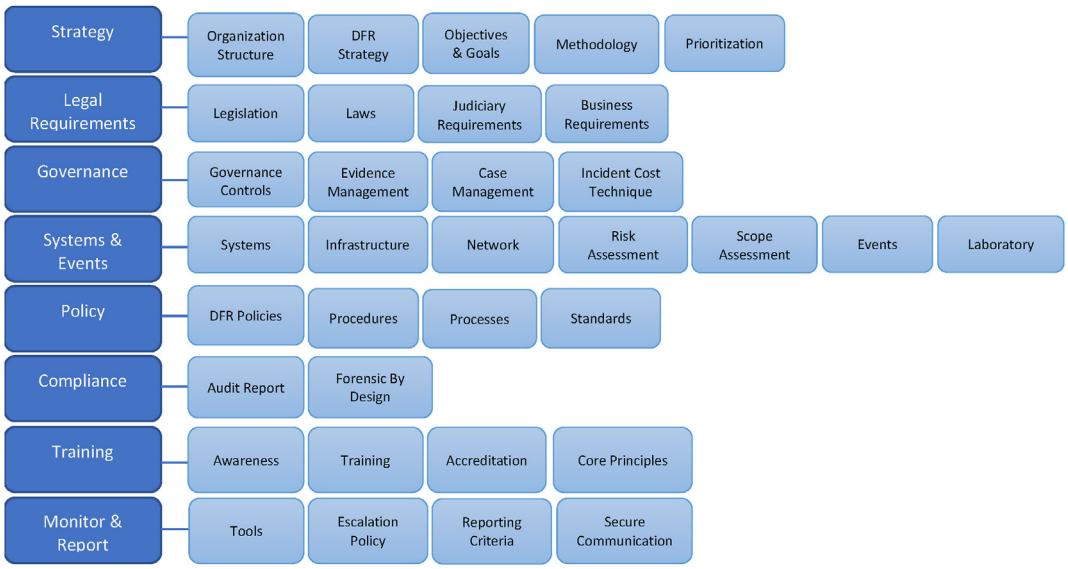

Fig. 3. Extended DFRCF with domains and sub domains (v1) – pre participant input.

learned in security incident response. The extended DFRCFv2 provides a comprehensive approach domain that entails additional domain/subs as follows: legal requirements, governance and training, as shown in Fig. 3. The following is a brief discussion of the extended DFRCFv2 domains, and how the domains satisfy the goals and objectives of a DFR model, when following up on security incidents and the model's effectiveness in practice, through practical validation.

3.1. Model development and design principles

Design principle is critical to model development (de Bruin et al., 2005; Maier et al., 2009; Becker et al., 2009; Solli-Sæther and Gottschalk, 2010; Pöppelbuß et al., 2011). For the purpose of this research, the following proposed design structures by De Bruin et al. (2005) and Pöppelbuß et al. (2011) are utilised.

According to De Bruin et al. (2005) a maturity model must have a purpose and that purpose might either be of a descriptive, prescriptive or comparative nature.

- A descriptive model is defined as a single point event that does not plot a path towards improving maturity, 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 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 utilised across industries. The model designed in this research is prescriptive because it has the ability to plot a maturity path and the domains are interrelated.

Table 2 illustrates the criteria and characteristics that a model must consider during its design. It also illustrates how this research

Table 2
Design principles criteria and characteristics.

Criterion	Characteristics	
Focus of Model	Domain Specific √	General
Prerequisites for applicability (Poppelbub et al. (2011)	Good understanding of Digital Forensic Readiness	
Purpose of use (Poppelbub et al. (2011)	To assist organization to gauge their level of maturity towards forensic readiness and thereby to provide a tool to examine the gap to a state of full	
Model differentiation (Poppelbub 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 √
	Executive, 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 Region) √	
Approach	Top-Down/Bottom-Up	
Maturity Levels and Definitions	Level 1: Non- Existent/See Appendix 2.1 & 2.2 Level 2: Basic/See Appendix 2.1 & 2.2 Level 3: Intermediate/See Appendix 2.1 & 2.2 Level 4: Advanced/See Appendix 2.1 & 2.2 Level 5: Full/See Appendix 2.1 & 2.2	

Table 3
IT practitioners interview statistics.

Interview	Invited for Interview	Confirmed Interview	Completed Interview
Number	20	13	10
Percent	100%	65%	50%
Interview Type	Face2Face	Online Skype	Total
Number	8	2	10
Percent	80%	20%	100%

applied the design principles. The design principles guide the designer through the different decision-making points (De Bruin et al., 2005; Pöppelbuß et al., 2011). The first consideration of the model is its focus; will the model be a general model or is the model designed for a specific domain. In this case the model is specific to DFR. Other key criteria that should be considered in the design process are who the stakeholders are, who the audiences are and how the model will be applied. This study employs a top-down approach: definitions of the maturity levels are developed first before measures are defined to fit the definitions (De Bruin et al., 2005).

The DFMM maturity model utilises five maturity levels namely Level 1: Non-Existent, Level 2: Basic, Level 3: Intermediate, Level 4: Advanced and Level 5: Full. The maturity levels are adaptations of the Data centric security model (Grandison et al., 2007; van Cleeff, 2008). Level 1 is included in this research to accommodate organisations that have not met all the conditions for level 2.

3.2. Data collection and sampling

The literature suggests the use of interviews, Delphi studies, case studies and focus groups to establish the characteristics of a maturity model (Pöppelbuß et al., 2011). These methods indicate the use of a qualitative approach (Raber et al., 2011). The literature discourages the use of quantitative methods for designing maturity models, this is 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 et al., 2002). This study employs purposive sampling, and structured and semi-structured interviews to collect data from DF practitioners/organisations who:

- Provide a financial service
- Have a digital forensic footprint
- Are willing and able to contribute to the research
- Are suitably knowledgeable about digital forensic readiness
- Are registered with the Financial Services Board (e.g., South African Reserve Bank)

3.3. Interview process

Based on the afore-stated constraints, this study interviewed ten participants that were selected using purposive random sampling. Details of how the interview was conducted is detailed in Table 3.

Participants were interviewed in their place of work on a pre-arranged day. Two open ended questions prompted discussions on DFR domains and maturity assessment model (See Appendix 3 for design instruments). Each of the interviews lasted between 7 and 36 min and were audio recorded with the consent of the participants. The conversations recorded were transcribed post interview via Atlas.ti software (See Appendix 3 for design instruments) using the Minnesota oral history association transcription conventions. The data was analysed and classified according to DRF domain themes and subsequently utilised to modify the design of the maturity model.

Henceforth, the main objectives of the interviews were:

- To validate the DFRCF v2 structure.
- To understand whether a checklist approach or a qualitative approach was more appropriate for the assessment model.
- To validate the DFMM maturity model matrix.

In addition, this study has investigated several DFR frameworks to determine the structure (domains and sub-domains) required to implement and manage DFR. This approach is supported by Kohn et al. (2006) who recommends that such a framework should be considered as a supporting structure for DFR. The criteria used for inclusion are that the framework must be; part of academic literature, applicable to computer or digital forensics and focussed on digital forensic *readiness*. The frameworks upon which this research is developed are:

- The DFR commonalities framework by Whyte and Claims (2012). This framework performs a comparative analysis on two popular frameworks (The Structured approach and the Ten Step process) to determine the domains and sub-domains of DFR. The DFRCF is included in the investigation conducted in this study because it already possesses the best aspects of DFR, that have been derived from the comparative study.
- The Barske et al. (2010) framework. This is similar to the DFRCF because both studies examine and incorporate findings as described in the unpublished article: "The case for digital forensic readiness" (Jordaan, 2009). The Barske et al. (2010) framework describes the aspects of DFR as well as organisational characteristics that are impacted by DFR.
- The digital forensic management framework (DFMF). This describes the goals, steps and deliverables of pro-DFR management that are able to assist organisations in the implementation of DFR (Grobler et al., 2010a).
- The integrated cloud incident handling and forensic-by-design model proposed by Ab Rahman et al. (2016). This model provides specific practices in a six-phase iterative approach. The phases are: Preparation (integrated with forensic readiness principles); Identification; Assessment (integrated with forensic collection and analysis practices); Action and Monitoring; Disaster recovery and management; and Evaluation (integrated with forensic presentation practices).

See appendix 1 for the DFRCF structure and interview questions and appendix 2.1 and 2.2 for the DFMM maturity model and interview questions.

4. Discussion of Findings

This section presents and discusses the results of the semi-structured interviews for both the DFRCFv2 structure and the DFMM Maturity assessment model. Table 4 displays the

Table 4
Participant demographics.

Participant	Years of Forensic experience	Industry where most forensic experience gained	Contributed Forensically to more than one industry	Size of Current Company	Highest Forensic Education	Board member of any organization in a forensic capacity	Have implemented forensic measures that are widely adopted by an organizations	Have recommended forensic measures that are utilised across industries
P1	5	Long Term insurance	Contributed to one insurance organization.	>10,000	B.Com Hons (Computer Forensics)	No	No	No
P2	8	Long Term insurance	Contributed to one insurance organization	15,000 staff in SA and 40,000 staff internationally	B.Com Hons (Computer Forensics)	No	Yes	No
P3	14	Financial Institution/ Banking	Yes, Banking	1001−5000	Mtech.	Yes	No	No
P4	20	Short Term insurance	Contributed to one insurance organization	>=2300	B.Com Hons (Computer Forensics)	Yes	No	No
P5	7	Not Available	Not Available	501−1000	B.Eng	No	No	No
P6	11	Banking	Not Available	1001−5000	MBA	No	No	No
P7	16	Law Enforcement	Yes, across several industries.	655	Msc	Association of Certified Fraud Examiner	Yes	Yes
P8	14	Public Sector, Mining	Yes: Oil & Gas, Public Sector, Technology, Gaming	Not Applicable(Currently retired)	B.Com Hons (Computer Forensics), CISSP	No	Built the forensic framework for a large financial services organization and done training for many organization across the globe	No
P9	>15	Industry & Academia	Published widely in academia	>=1000-2000	PhD	Not Applicable	Yes	Yes
P10	14	Long Term insurance	No	3000	Diploma in Criminal Justice & Forensic Auditing	No	Yes, one organization	No

demographics of the participants. The table shows the industries in which they operate, their forensic experience, the size of the organization, their highest forensic qualification, and so on. 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.

4.1. DFRCF domains and sub domains (DFR structure)

4.1.1. Strategy domain

Six of the participants agreed completely with the domain contents and did not propose any changes. The participant from the public sector suggested that the sub domains: *DFR strategy* and *methodology* be combined and renamed *Strategic framework*. This study accepted the proposed name change, because it encapsulates the intent: mandating the organisation to strategically operate its forensic capabilities within the proposed framework.

4.1.2. Legal domain

The discussions relating to this domain elicited a variety of responses, but the majority of participants felt that the original content was sufficient. However, this study noted that participant seven (who has several DFR publications and who practices in the public sector) disagreed strongly with the majority of participants. The participant argued that the three sub domains: *laws, legislation* and *regulations* were not entirely relevant in the South African context. *Legislation* was renamed *Statutory laws*; *Laws* was renamed *Common law* and *Judiciary requirements* was renamed *Case law*. Participants 1 and 2 suggested that this domain must incorporate regulations impacting DFR, such as the electronic communications policy or the Payment Card Industry Data Security Standard. This study accepted the inclusion of the *Regulation* sub domain and the name changes suggested by participant seven.

4.1.3. Governance

The participants could only find agreement on two sub domains, namely the *Governance controls* and *Evidence management*. Several other sub domains were however introduced such as, *Risk assessment, Audit report* and *Incident management*. These three new additions were suggested unanimously by the three participants who are the only forensic consultants in the group. The *Incident cost techniques* sub domain was renamed *Incident management*. The previous name was too granular and conveyed the understanding that the cost technique was the only item under discussion. Participants suggested that there are more underlying activities such as deciding "*what needs to happen and when*", amongst others. This study has extended the *Governance* domain and the final version is depicted by Fig. 4.

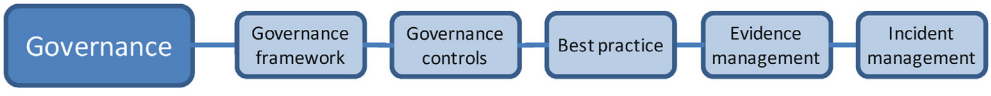

Fig. 4. Governance domain and elements.

Table 5
Policy & procedure 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					

Table 6
New domains and sub domains suggested by participants.

New Main Domain Name	New Sub-Domains (Elements) Introduced	Participant
Group Support	Exco buy-inn	P1, P2
Lab Management	Copies & 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

4.1.4. Systems and events

The prevailing sentiment was that Infrastructure, Network, Systems, Events and Laboratory must remain within the domain. Thus, the domain remains largely unchanged except for the removal of the *Risk assessment* sub domain and the name change of the *Laboratory* sub domain to *DF capacity*. Participant seven argued that laboratories are mainly utilised in large organisations and that this term 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 refer to a facility.

4.1.5. Policy

The participants initiated several changes to this domain. There was no general consensus and therefore Table 5 illustrates all the sub domain elements proposed by the participants (see Table 6).

It is impractical to display this level of detail, as proposed by the various responses, in the 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 policies as *Policy*. This study utilised the above groupings to populate the *Policy* domain and accepted it as the final structure of this domain.

4.1.6. Compliance

Most participants agreed that the DFRCF must contain a *Compliance* domain. However, participants 3 and 6 argued that the *Compliance* domain should be integrated as a sub domain under the *Governance* or the *Legal requirements* domains. A new sub domain was introduced, namely *Compliance report* and the name of the *Audit report* sub domain was shortened to *Audit* sub domain. The reason for the name change was that the *Audit* sub domain was viewed as the activity and the *Compliance report* sub domain was the output. 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).

Table 7
Responses to the two approaches.

Approach	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10
Tick Box, Bullet Point Qualitative (words)			√	√	√				√	√
Combination Approach	√	√					√	√		

4.1.7. Training

The training domain is uncomplicated, and all participants accepted the proposed model. There were two suggestions to rename the *Training* sub domain to *Forensic training* and *Investigative training*, from participant 7 and participant 3, respectively. This study accepted the name change to *Forensic training* as the change clarifies the intent of the sub domain.

4.1.8. Monitor and report

This study initially proposed 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 as such the *Escalation policy* sub domain was removed from this domain to the *Policy* domain. However, this left a gap as this domain required an action that ensures there is an escalation process, as certain incidents must be forwarded for formal investigations based on the triggers created. 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 the "*what*" and "*when*" (escalation criteria), and the "*how*" (escalation policy).

4.2. Proposed hierarchy framework

Six (6) participants, including a forensic practitioner in the banking industry, suggested a hierarchical structure based on the Plan, Do, Check, Act cycle. This cycle of continuous process improvement postulated by Deming, (1982) and in agreement with Rowlingson (2004), can be utilised in the DFRCF in the following manner: 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. This study believes that such a structure will assist organisations in organising and prioritising actions for DFR implementation (see Fig. 5).

Fig. 5. Refined domains of DFRCF- v2.

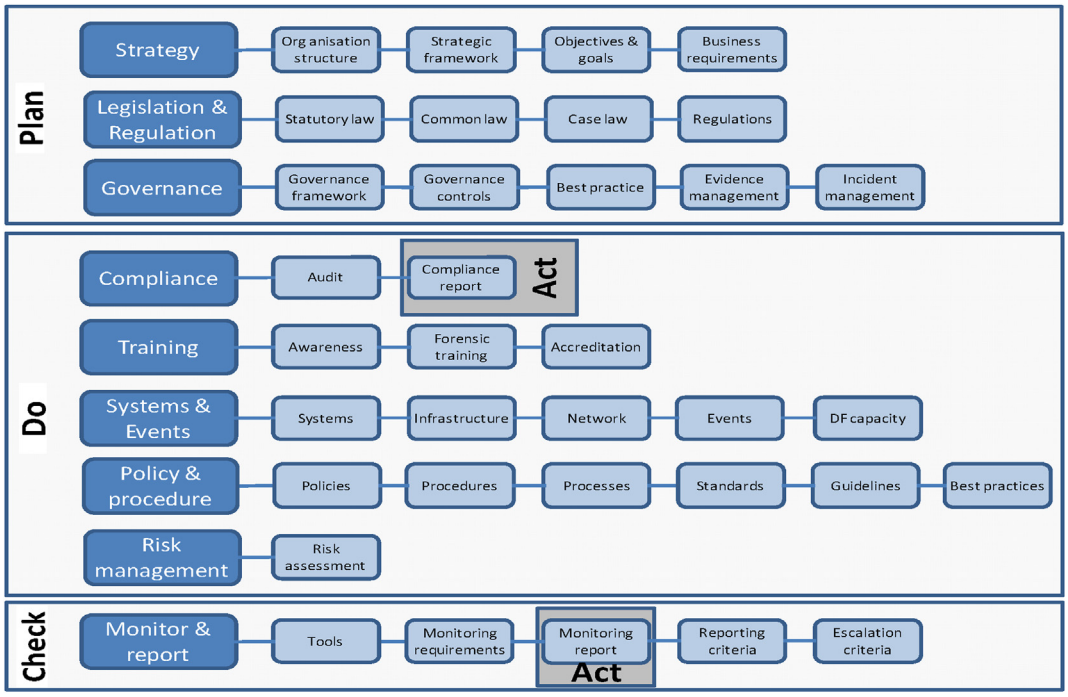

Fig. 6. DFRCFv2 (DFMM) – post practitioner input.

4.2.1. Proposed domains

This study proposed eight domains (as part of the extended DFRCF-v1) and five new domains were proposed by the participants during the interviews. The proposed domains and sub domains are reflected in Table 5. Since nearly all the proposed domain elements are already resolved within the DFRCF v1 (Fig. 3), Outcome from the interview were fused into extended DFRCF-v1 to produce the final DFRCF v2 as presented in with the addition of *Risk management* Fig. 6.

4.3. Maturity assessment model

The participants had varied responses to the selection of the assessment approach, as illustrated by Table 7.

Half (5) of the participants preferred the tick box 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 to a range of interpretations and the tick box approach gives a clearer indication of what is under scrutiny. Four participants selected a combination of both the qualitative and tick box approach. This means that a third approach was proposed by the participants. This new combination approach was selected by participants in the insurance and private consultancy industries. Participant six, from the banking industry was the only respondent, who opted for the qualitative approach, citing: "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 tick box approach stifles out-of-the-box thinking and as such will cause certain information to be overlooked.

This study accepts the check-list approach model (see appendix 2.1) 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 have been defined with the input of the forensic practitioners, thus strengthening the validity of the approach followed to define the maturity levels. 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 (see appendix 2.1). This is to illustrate that the maturity levels are applicable to every domain and sub domain. There are 5 levels of maturity in the model. The model is read from left to right, in a horizontal direction. 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 not a level lower than level 1.

4.4. The Extended Digital Forensics Readiness Commonalities Framework (DFRCF)

In this section, we propose the main output of this study. The Extended Digital Forensics Readiness Commonalities Framework (DFRCF) is intended to enable organisations implement and manage their DFR programmes as it illustrates the scope of DFR and fosters the benefits of DFR.

4.5. Limitations and future research

The limitation of this study is that only 10 participants were interviewed, as such it is possible that not all the aspects of DFR were revealed. For example, the study has not had clarity regarding the various roles within DFR; neither does the implication of collecting private information emerge. Another limitation is that the models still require further testing in practice before they can be generalised (Karokola et al., 2013). On the other hand, organisations have been presented with a framework and an assessment model that will enable them to start the conversation of readiness assessment, without which, organisations will fail to identify the potential DFR risks and opportunities exposed by an assessment. Furthermore, future studies can consider a non-checklist approach to model validation. In addition, future research could compare responses between organizations/practitioners who have implemented forensic measures that are widely adopted by an organization and those who have not.

5. Conclusion

Organisations that do not have a means to measure their security mechanism and forensic readiness run the risk of economic crime exploitation in the current century (Ayangbekun et al., 2014). This study examined current literature to understand the DFR structure and how such a structure can be used to design a maturity assessment model. The structure became apparent from literature and a qualitative approach was used to test the DFR structure with forensic practitioners. The respondents shaped the structure, and the domains were used to create a maturity assessment model. Two approaches were presented to participants, however a third response, which is a combination of check list and qualitative narration, was proposed by the respondents.

The refined structure (domains and sub domains) is illustrated in Fig. 6. The figure demonstrates the scope and structure of DFR and as such is useful to financial services organisations that invest in DFR. The figure illustrated is the extended DFRCFv2 framework and it mimics the Deming lifecycle: Plan, Do, Check and Act. This is the updated product of the extended DFRCF developed in this research which subsequently present this framework to the academic world and to the forensic practitioners. This framework conforms not only to approved industry standard principles and guidelines towards forensic readiness, many of which are captured in the Rowlingson (2004) report on Forensic Readiness, but also with the proposed NIST cybersecurity framework as shown in Sedgewick (2014). This research utilized the check-list approach, the preferred choice of the majority of the participants.

The refined DFR maturity assessment model is illustrated in appendix 2.1. 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 at achieving a maturity rating of *5*. Future iterations of this refined model should incorporate perspectives from more practitioners who have experience dealing with major incidents and can provide additional insights into forensic preparedness requirements.

Declaration of competing interest

No Conflict of Interest. This article is an updated version of research conducted.

Appendix A. Supplementary data

Supplementary data to this article can be found online at https://doi.org/10.1016/j.fsidi.2022.301348.

Wilsdon & Slay (2005). Digital Forensics: Exploring Validation, Verification & Certification. *Proceedings of the First International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE'05)*, 7–9 November 2005, pp. 48–55.

References

Ab Rahman, N.H., Choo, K.K.R., 2015. A survey of information security incident handling in the cloud. Comput. Secur. 49, 45–69.

Agarwal, A., Gupta, M., Gupta, S., Gupta, S.C., 2011. Systematic digital forensic investigation model. Int. J. Comput. Sci. Secur. 5 (1), 118–131.

Agerfalk, P.J., Conboy, K., Myers, M.D., 2020. Information systems in the age of pandemics: COVID-19 and beyond. Eur. J. Inf. Syst. 29 (3), 203–207. Business Process Management and Digital Innovation.

Alenezi, A., Hussein, R.K., Walters, R.J., Wills, G.B., 2017a. A framework for cloud forensic readiness in organizations. In: 5th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud), San Francisco, CA, 2017, pp. 199–204.

Alenezi, A., Zulkipli, N., Atlam, H., Walters, R., Wills, G., 2017b. The impact of cloud forensic readiness on security. In: Proceedings of the 7th International Conference on Cloud Computing and Services Science. CLOSER 2017, pp. 511–517.

Arde, A., 2012. November 17). Hack Attack a Costly Lesson for Banks. The Independent on Saturday.

Ariffin, K.A.Z., Ahmad, F.H., 2021. Indicators for maturity and readiness for digital forensic investigation in era of industrial revolution 4.0. Comput. Secur. 105. https://doi.org/10.1016/j.cose.2021.102237.

Ayangbekun, O.J., Bankole, F.O., Saka, B.A., 2014. Analysis of security mechanism in Nigeria E-banking platform. Int. J. Electrical Comput. Eng. I 4 (1), 837–847, 6.

Baror, S.O., Venter, H., 2019. A Taxonomy for cybercrime attack in the public cloud. In: International Conference on Cyber Warfare and Security. Academic Conferences International Limited, p. 505.

Baror, S.O., Venter, H.S., Adeyemi, R., 2020. A natural human language framework for digital forensic readiness in the public cloud. Aust. J. Forensic Sci. 1–26.

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 (ISSA), Johannesburg, pp. 1–6, 2-4 August.

Baskerville, R.L., Kaul, M., Storey, V.C., 2015. Genres of inquiry in design-science research: justification and evaluation of knowledge production. MIS Q. 39 (3), 541–564.

Becker, J., Knackstedt, R., Pöppelbuß, J., 2009. Developing maturity models for it management – a procedure model and its application. Bus. Inf. Syst. Eng. (BISE) 1 (3), 213–222.

Bonazzi, R., Hussami, L., Pigneur, Y., 2010. Compliance management is becoming a major issue in IS design. Inf. Syst.: People Organ. Inst.Technol. 391–398.

Bradford, P., Brown, M., Perdue, J., Self, B., 2004. Towards proactive computer-system forensics. Proc. Inf. Technol.: Coding Comput. ITCC 648–652, 5-7 April.

Chernyshev, M., Zeadally, S., Baig, Z., 2019. Healthcare data breaches: implications for digital forensic readiness. J. Med. Syst. 43 (1).

Cichonski, P., Millar, T., Grance, T., Scarfone, K., 2012. Computer security incident handling guide. NIST - Spec. Publ. 800 (61), 1–147.

Cram, W.A., Proudfoot, J.G., D'Arcy, J., 2017. Organizational information security policies: a review and research framework. Eur. J. Inf. Syst. 26 (6), 605–641.

De Bruin, T., Freeze, R., Kaulkarni, U., Rosemann, M., 2005. Understanding the main phases of developing a maturity assessment model. In: *Australasian Conference On Information Systems (ACIS)*, Australia. New South Wales, Sydney, 30 November – 2 December.

Deming, W.E., 1982. Out of the crisis, MIT center for advanced engineering study, Boston, MA.Emerald. (2013). How To Research. http://www.emeraldinsight.com/research/guides/index.htm.

Dykstra, J., Sherman, A.T., 2011. Understanding issues in cloud forensics: two hypothetical case studies. Annual ADFSL Conference on Digit. Forensics Secur. Law 10.

Fraser, P., Moultrie, J., Gregory, M., 2002. The use of maturity models/Grids as a tool in assessing product development capability. In: Proceedings of the IEEE International Engineering Management Conference. IEMC 2002, Cambridge, UK, pp. 244–249.

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. In: Proceedings of the 2007 2nd IEEE/IFIP International Workshop on Business-Driven IT Management (BDIM), pp. 84–93, 21 May 2007.
Grispos, G., Glisson, W.B., Storer, T., 2017. Enhancing security incident response follow-up efforts with lightweight agile retrospectives. Digit. Invest. 22 (1), 62–73.
Grobler, C.P., Louwrens, C.P., Von Solms, S.H., 2010a. A framework to guide the implementation of Proactive Digital Forensics in organisations. In: 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. In: Proceedings of the '10 International Conference on Availability, Reliability, and Security (ARES), Krakow, 15 February -18 February, pp. 647–652.
Henderson, J.C., Venkatraman, N., 1993. Strategic alignment: leveraging information technology for transforming organizations. IBM Syst. J. 32 (1). https://doi.org/10.1147/sj.382.0472.
Iqbal, A., Ekstedt, M., Alobaidli, H., 2018. Digital forensic readiness in critical infrastructures: a case of substation automation in the power sector. In: Matoušek, P., Schmiedecker, M. (Eds.), Digital Forensics and Cyber Crime. ICDF2C 2017. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, 216. Springer.
Johnson, C., Badger, M., Waltermire, D., Snyder, J., Skorupka, C., 2016. Guide To Cyber Threat Information Sharing. No. NIST Special Publication (SP) 800-150 (Draft). National Institute of Standards and Technology.
Jordaan, J., 2009. The Case for Digital Forensic Readiness. University of Cape Town. Unpublished paper.
Kang, M., Hovav, A., 2020. Benchmarking methodology for information security policy. (BMISP): artifact development and evaluation. Inf. Syst. Front 22, 221–242.
Karie, N.M., Karume, S.M., 2017. Digital forensic readiness in organizations: issues and challenges. J. Digit. Forensics Secur. Law: JDFSL 12 (4), 43–53, 2017.
Karokola, G., Kowalski, S., Yngström, L., 2013. Evaluating A framework for securing e-government services – a case of Tanzania. In: Proceedings of the 2013 46th Hawaii International Conference on System Sciences, Johannesburg, South Africa. ISBN: 978-1-.
Kebande, V.R., Venter, H.S., 2019. A comparative analysis of digital forensic readiness models using CFRaaS as a baseline. Wires Forensic Sci. J. 1 (6). https://doi.org/10.1002/wfs2.1350.
Kempen, A., 2017. Cybersecurity in South Africa - are there lessons to be learned from the major data breach? Servamus Community Based Safety Secur. Mag. 110 (12), 16–19.
Kochan, A., 1993. Internal evaluations. TQM Mag. 5 (2).
Kohn, M., Eloff, J.H.P., Olivier, M.S., 2006. Framework for a digital forensic investigation. In: 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.
Le, N.T., Hoang, D.B., 2017. Capability maturity model and metrics framework for cyber cloud security. Scalable Comput. 18 (4), 277–290.
Luftman, J.N., Lewis, P.R., Oldach, S.H., 1993. Transforming the enterprise: the alignment of business and information technology strategies. IBM Syst. J. 32 (1).
Maier, A.M., Moultrie, J., Clarkson, P.J., 2009. Developing maturity grids for assessing organisational capabilities: practitioner guidance. In: Proceedings of the 4th International Conference on Management Consulting, Academy of Management (MCD). Vienna, Austria, 11–13 June 2009.
Markus, M.L., Majchrzak, A., Gasser, L., 2002. A design theory for systems that support emergent knowledge processes. MIS Q. 179–212.
Marshall, A.M., 2011. Standards, regulation & quality in digital investigations: the state we are in. Digit. Invest. 2 (8), 141–144.
Martini, B., Choo, K.-K.R., 2012. An integrated conceptual digital forensic framework for cloud computing. Digit. Invest. 9 (2), 71–80.
Mavroeidis, V., Bromander, S., 2017. Cyber threat intelligence model: an evaluation of taxonomies, sharing standards, and ontologies within cyber threat intelligence. In: 2017 European Intelligence and Security Informatics Conference (EISIC). IEEE, pp. 91–98.
Mettler, T., 2011. Maturity assessment models: a design science research approach. Int. J. Soc. Syst. Sci. 3 (1/2), 81–98.
Niekerk, V.B., 2017. An analysis of cyber-incidents in South Africa. Afr. J. Inf. Commun. (AJIC) 20, 113–132. https://doi.org/10.23962/10539/23573.
Njenga, K., Brown, I., 2012. Conceptualizing improvisation in information systems Security. Eur. J. Inf. Syst. 21 (6), 592–607.
Pangalos, G., Katos, V., 2010. Information assurance and forensic readiness. Lecture notes of the institute for computer sciences. Soc. Inf. Telecommun. Eng. 26, 181–188.
Pangalos, G., Ilioudis, C., Pagkalos, I., 2010. The importance of Corporate Forensic Readiness in the information security framework. In: *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.
Park, S., Kim, Y., Park, G., Na, O., Chang, H., 2018. Research on digital forensic readiness design in a cloud computing-based smart work environment. Sustainability 10 (4), 1203.
Pilli, E.S., Joshi, R.C., Niyogi, R., 2010. Network forensic frameworks: survey and research challenges. Digit. Invest. 7 (1), 14–27.
Pollitt, M., Casey, E., Jaquet-Chiffelle, D., Gladyshev, P., 2018. A Framework for Harmonizing Forensic Science Practices and Digital/Multimedia Evidence the Organization of Scientific Area Committees for Forensic Science. OSAC), USA, 2018.
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. In: Proceedings of the 19th European Conference on Information Systems (ECIS). Helsinki, Finland.
Posey, C., Raja, U., Crossler, R.E., Burns, A.J., 2017. Taking stock of organizations' protection of privacy: categorizing and assessing threats to personally identifiable information in the USA. Eur. J. Inf. Syst. 26 (6), 585–604.
Quick, D., Choo, K.K.R., 2018. Digital forensic intelligence: data subsets and Open Source Intelligence (DFINT+ OSINT): a timely and cohesive mix. Future Generat. Comput. Syst. 78, 558–567.
Raber, D., Winter, R., Wortmann, F., 2012. Using quantitative analyses to construct a capability maturity model for business intelligence. In: Proceedings of the 2012 45th Hawaii International Conference on System Sciences, Maui, Hawaii, pp. 4219–4228, 4-7 January 2012.
Ramirez, T.M., 2002. You can't manage what you don't measure. Measuring project performance. http://www.pmipr.org/html/Presentaciones/You%20Cant%20Manage%20What%20You%20Dont%20Measure.pdf. (Accessed 10 September 2013).
Rege, M., Mbah, R.B.K., 2018. Machine learning for cyber defense and attack. In: Proceedings at the Seventh International Conference on Data Analytics. Athens, Greece.
Reith, Mark, Carr, Clint, Gregg, Gunsch, 2002. An examination of digital forensic models. Int. J. Digit. Evid. 1 (3), pp1–pp12.
Rid, T., Buchanan, B., 2015. Attributing cyber attacks. J. Strat. Stud. 38 (1–2), 4–37.
Rowlingson, R., 2004. A ten step process for forensic readiness. Int. J. Digit. Evid. 2 (3), 1–28.
Sachowski, J., 2016. Investigative process models. In: Implementing Digital Forensic Readiness: from Reactive to Proactive Process. Elsevier.
Sedgewick, A., 2014. Framework for Improving Critical Infrastructure Cybersecurity version 1.0 (No. NIST-Cybersecurity Framework).
Siponen, Mikko, Iivari, Juhani, 2006. Six design theories for IS security policies and guidelines. J. Assoc. Inf. Syst. 7, 445–473.
Solli-Sæther, H., Gottschalk, P., 2010. The modeling process for stage models. J. Organ. Comput. Electron. Commer. 20 (3), 279–293.
Spruit, M., Röling, M., 2014. ISFAM: the information security focus area maturity model. Proc. Eur. Conf. Inf. Syst.
Wilsdon, T., Slay, J., 2005. Digital forensics: exploring validation, verification and certification. In: First International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE'05), pp. 48–55.
Wu, T., Disso, J.F., Jones, K., Campos, A., 2013. Towards a SCADA forensics architecture. In: 1ST International Symposium for ICS& SCADA Cyber Security Research Proceedings, pp. 1–12.
Tan,J.(2001). Forensic readiness. http://www.atstake.com/research/reports/acrobat/atstakeforensic_readiness.pdf"_forensic_readiness.pdf.
Teing, Y.-Y., Ali, D., Choo, K.-K.R., Yang, M., 2016. Forensic investigation of P2P cloud storage services and backbone for IoT networks: BitTorrent Sync as a case study. Comput. Electr. Eng. https://doi.org/10.1016/j.compeleceng.2016.08.020.
Valjarevic, A., Venter, H.S., 2011. Towards a digital forensic readiness framework for public key infrastructure systems. In: 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. Inf. Secur. Tech. Rep. 3 (3), 112–117. ISSN 1363-4127.
Verma, R., Govindaraj, J., Chhabra, S., Gupta, G., 2019. DF 2.0: an automated, privacy. Preserving, and efficient digital forensic framework that leverages machine learningfor evidence prediction and privacy evaluation. J. Digit. Forensics Secur. Law 14 (2), 1–12.
Weiss, N., Miller, R.S., 2015. The target and other financial data breaches: the congressional research service. Retrieved from. https://fas.org/sgp/crs/misc/R43496.pdf. on 01/05/2021.
Whyte, G., Claims, I., 2012. The state of digital forensic readiness of financial services companies in South Africa. In: Proceedings of the 3rd International Conference on Information Management and Evaluation (ICIME) 2012, 16-17 April 2012, Ankara, Turkey, pp. 284–299.