Digital Forensic Readiness: Expert Perspectives on a Theoretical Framework

Article *in* Computers & Security · April 2015

DOI: 10.1016/j.cose.2015.04.003

CITATIONS
36

READS
2,319

4 authors, including:

Atif Ahmad
University of Melbourne
97 PUBLICATIONS **1,518** CITATIONS
SEE PROFILE

Sean B. Maynard
University of Melbourne
74 PUBLICATIONS **1,332** CITATIONS
SEE PROFILE

Andrew Lonie
University of Melbourne
78 PUBLICATIONS **2,513** CITATIONS
SEE PROFILE

Digital Forensic Readiness: Expert Perspectives on a Theoretical Framework

COMPUTERS & SECURITY 52 · APRIL 2015
DOI: 10.1016/j.cose.2015.04.003
Mohamed Elyas, Atif Ahmad, Sean B. Maynard & Andrew Lonie

Digital Forensic Readiness: Expert Perspectives on a Theoretical Framework

Mohamed Elyas[1]
Atif Ahmad[1]
Sean B. Maynard[1*]
Andrew Lonie[2]

[1]Department of Computing and Information Systems
Melbourne School of Engineering
University of Melbourne
Victoria, Australia

[2]Victorian Life Sciences Institute (VLSI)
University of Melbourne
Victoria, Australia

*Corresponding Author Details
Email: sean.maynard@unimelb.edu.au

Phone: +61 3 8344 1573

Abstract

Modern organizations need to develop 'digital forensic readiness' to comply with their legal, contractual, regulatory, security and operational obligations. A review of academic and practitioner literature revealed a lack of comprehensive and coherent guidance on how forensic readiness can be achieved. This is compounded by the lack of maturity in the discourse of digital forensics rooted in the informal definitions of key terms and concepts. In this paper we validate and refine a digital forensic readiness framework through a series of expert focus groups. Drawing on the deliberations of experts in the focus groups, we discuss the critical issues facing practitioners in achieving digital forensic readiness.

Keywords

Digital Forensics; Digital Forensic Readiness; Information Security Management; Focus Group

1. INTRODUCTION

Organizations are increasingly reliant upon information systems for almost every facet of their operations. As a result, there are legal, contractual, regulatory, security and operational reasons why this reliance often translates into a need to conduct digital forensic investigations (Rowlingson, 2004). However, conducting digital forensic investigations and collecting digital evidence is a specialized and challenging task exacerbated by the increased complexity of corporate environments, diversity of computing platforms, and large-scale digitisation of businesses (Taylor et al., 2010). There is agreement in both professional and academic literature that in order for organizations to meet this challenge, they must develop 'digital forensic readiness' – the proactive capability to collect, analyse and preserve digital information (Grobler et al. 2010). Unfortunately, although digital forensic readiness (DFR) is becoming a legal and regulatory requirement in many jurisdictions in the western world, studies show that most organisations especially in Australia have not developed a significant capability in this domain (e.g. the Australian Institute of Criminology reports that less than 2% of Australian organizations have a plan for digital forensics, see AIC (2009)).

A key issue facing organizations intending to develop a forensic readiness capability is the lack of comprehensive and coherent guidance on how forensic readiness can be achieved in both the professional and academic literature (Mouhtaropoulos, Li, & Grobler, 2014). A review of the literature conducted as part of this study found that the academic and professional discourse in forensic readiness is fragmented and dispersed in that it does not build cumulatively on prior knowledge (Elyas et al. 2014). Further, there is a lack of maturity in the discourse that is rooted in the reliance on informal definitions of key terms and concepts. For example, there is little discussion and understanding of the key organizational factors that contribute to forensic readiness, the relationships between these factors and the precise definitions including the scope and boundaries of these factors. Importantly, there is no collective agreement on the primary motivating factors for organizations to becoming forensically ready (Elyas et al., 2014).

Therefore, this research project proposes the following research question: *How can forensic readiness be achieved by organisations?*

This paper builds on our previous work published in Elyas et al. (2014) where we presented a DFR framework that explains the factors underpinning an organization's ability to meet its forensic objectives. The framework was based on a comprehensive analysis of literature since the term 'digital forensic readiness' was first introduced by Tan (2001).

In this paper, we validate and refine the framework through a series of three focus groups. We report on the views of experts with respect to the framework focusing on the points of agreement and disagreement. The outcome of this study is a complete and comprehensive set of factors that comprise digital forensic readiness, and a comprehensive list of organizational forensic readiness objectives. Organizations can use this framework in the assessment and improvement of their digital forensic readiness.

The structure of this paper is as follows. In the background section we discuss previous work on digital forensics and DFR followed by a review of the DFR framework described in Elyas et al. (2014). We then describe the research method used in this study followed by the findings from the focus groups. This is followed by a discussion of the various perspectives of the experts on the topic of DFR and our framework. The following section provides insights on the use of focus groups and explains how they add strength to this study. Finally, we discuss the contributions to practice arising from the validated framework.

2. BACKGROUND: DIGITAL FORENSIC READINESS

Digital forensic readiness (DFR) was first described by Tan (2001) as setting up digital forensics in organizations to minimize the cost of digital forensics whilst maximizing the capability of an organization to collect legally reliable digital evidence. Pangalos and Katos (2010) extend this perspective defining forensic readiness as "*the state of the organization where certain controls are in place in order to facilitate the digital forensic processes and to assist in the anticipation of unauthorized actions shown to be disruptive to planned operations*". Forensic readiness, as per this definition, would facilitate the entire forensic process rather than only focusing on the production of credible digital evidence and adds an 'anticipatory' dimension to the forensic process.

Forensic readiness has been studied from many perspectives including resourcing (Reyes & Wiles, 2007), technology use and selection (Carrier & Spafford, 2003), training (Carrier & Spafford, 2003; Rowlingson, 2004), legal investigations (Casey, 2005), and policy (Yasinsac & Manzano, 2001). None of this research discusses forensic readiness holistically; rather, they each treat forensic readiness from their particular perspective. As organizations become more subject to regulation (e.g. Sarbanes-Oxley) the importance that is placed on being forensically ready is increasing (Marcella Jr., 2008) and therefore focusing on a comprehensive forensics readiness perspective becomes more important. But organizations need to be able to balance the cost of being forensically ready and the benefit of being able to produce digital forensic evidence as required for forensic readiness to be effective (Reyes & Wiles, 2007; Rowlingson, 2004).

Forensic readiness can be divided into operational readiness and infrastructural readiness (Carrier & Spafford, 2003). Operational readiness is concerned with the provision of training and equipment for individuals who are involved in forensics, whereas, infrastructural readiness is concerned with ensuring that the data of an organization is appropriately preserved. These concepts are also discussed by Rowlingson (2004) who proposes that activities such as: planning, policing, training, and monitoring elements are important to improve forensic readiness. Grobler et al. (2010) suggest that DFR is a proactive forensic activity. They also propose that cultural and governance aspects should be incorporated within forensic readiness, linking digital forensic readiness to organizational management.

As a whole, these studies give much guidance to organizations about becoming forensically ready. However, the individual studies focus only on their particular areas within forensic readiness, and as such the guidance to organizations seems to be ad-hoc and incomprehensive.

In our previous work (Elyas et al. 2014) we develop an initial framework for digital forensic readiness. The framework consists of: 1) a set of *Forensic Factors* that are concerned with the various areas of forensic readiness; and 2) a set of *Forensic Readiness Capabilities* that organizations aim to achieve (Figure 1). The components in the initial framework, including the *Forensic Factors*, *Forensic Readiness Capabilities* and all of the relationships, are defined from literature (see Appendix 1).

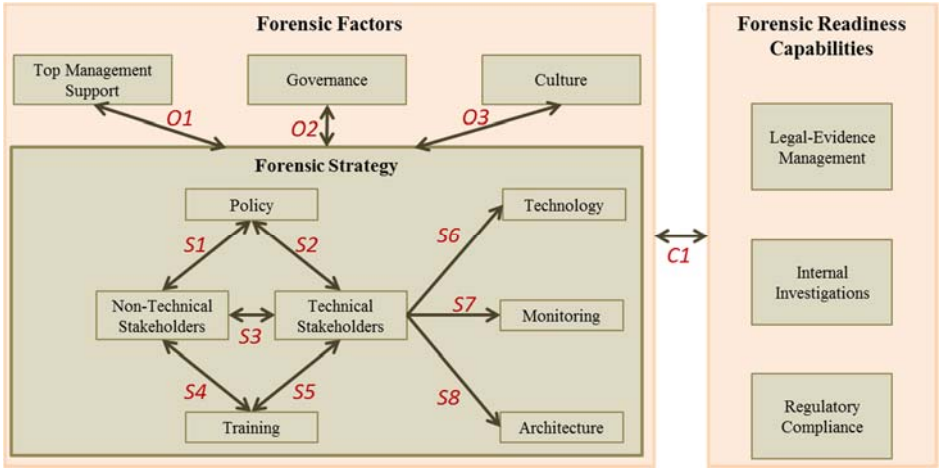

Figure 1: Digital Forensic Readiness (DFR) Framework (Elyas et al. 2014)

3. RESEARCH METHOD

A Focus Group is a "*research technique that collects data through group interaction on a topic determined by the researcher*" (Morgan, 1996) which capitalizes on communications between the participants to generate ideas (Kitzinger, 1995). Over the last 25 years, focus groups have been used extensively by researchers in

Information Systems (Belanger, 2012). The advantage of using focus groups over individual interviews is that a group discussion can occur that cause group participants to interact and reflect on each other views (Krueger & Casey, 2001), which in turn is likely to result in a better quality data. Further, the dynamics of a group discussion encourage the participants to discuss the issues of significance to them, using their own terminology, developing their own questions, which may take the research into a new direction – uncovering hidden areas of knowledge (Kitzinger, 1995). Krueger and Casey (2001) recommend holding three to four focus groups and suggested that theoretical saturation occurs within this range. There is also agreement that ideally focus groups should contain between four to eight participants (Kitzinger, 1995; Krueger & Casey, 2001).

In this research we conducted three focus groups comprised of participants with digital forensic experts from business, academic, consultancy, law enforcement, and military backgrounds. We invited 6 participants to each focus group and averaged between three and five participants with eleven experts in total (see Table 1 for a summary of participants).

Table 1 – Summary of Participants

Code	Focus Group	Industry	Staff Size	Position	Forensic Experience
Expert_1	1	Law Enforcement (Police)	10,000+	Digital Forensic Analyst Team Leader	4+ Years
Expert_2	1	Consultancy (Major Accountancy Firm)	10,000+	Director, Forensic Technology	9+ Years
Expert_3	1	Business (Gold Industry)	10+	Director, Business Owner	4+ Years
Expert_4	2	Consultancy / Law Enforcement	Multiple companies	Director, Forensic Technology	7+ Years
Expert_5	2	Education	5,000+	Professor	8+ Year
Expert_6	2	Business / Law Enforcement	10,000+	Technical Security Leader	5+ Years
Expert_7	2	Consultancy	10,000+	Advisory Senior Associate	7+ Years
Expert_8	2	Consultancy / Law Enforcement	10,000+	Senior Consultant	5+ Years
Expert_9	3	Consultancy / Law Enforcement / Army	300+	National Director - Forensic Technology	20+ Years
Expert_10	3	Consultancy	3,000+	Senior Manager	5+ Years
Expert_11	3	Education	5,000+	Academic	2+ Year

The purpose of the focus groups was to refine and validate our DFR framework. This project used an emergent approach, where the focus group questions were adapted across the focus groups and within the individual focus groups based on the direction of the study (in line with Morgan's (1996) approach). Subsequently, different sets of questions were used (see Appendix 2). Each focus group session was two-hours long and was moderated by one of the senior researchers. The sessions each comprised of three phases: 1 – capture the understanding of participants about forensic readiness, 2 – discuss aspects of the framework with the purpose of refining the framework, 3 – present the framework and then get participant reactions to it.

The rigor of analysis in focus groups has been classified into four categories (Krueger & Casey, 2001). In this research we use the most rigorous of the four categories: a complete transcript of each focus group's recording was made (over 42000 words in total). The observers (other researchers) also made notes of the important ideas in the discussion. At the immediate conclusion of each focus group, the researchers met to discuss the preliminary outcomes of the session. The analysis is based on a combination of this data, in addition to the data written by the participants in the second and third focus groups.

The focus group data was analysed using content analysis as described by Elo and Kyngäs (2008). Since the purpose of our study is to refine and test the DFR framework, a deductive content analysis approach has been adopted. The identified forensic readiness objectives and factors along with their properties formed a categorization matrix. The transcripts were carefully reviewed using an unconstrained coding approach where headings and notes were added to data. This was done to ensure that no important ideas discussed by the participants were overlooked. Next, the categorization matrix was used to map the headings from the text to the DFR framework. All comments that are related to a specific category were placed in their corresponding areas in the categorization matrix. The comments were compared with the categories to see what the participants

exactly thought. A comment may support the category, disagree with the category, or extend its sub-categories. After the components of the framework have been tested, the free-categories that do not correspond to any category in the categorization matrix were examined to decide whether they can be related to the research questions, or if they can add new insights to the framework.

Focus group validity can be assured through a combination of external validity (generalizability), internal validity (reliability), and relevance (realism) (Belanger, 2012). Belanger (2012) argues that analytical generalizability is achievable in focus groups, as the members of the groups are experts in the area, and therefore if well-selected, their views will be representative of the views of their peers in the same area. In this study we have used digital forensic experts, with reasonable experience, who were carefully selected so that their views were likely to be representative, and thus generalizable. Reliability of the study is achieved through thoroughly describing the focus group process from design to analysis, ensuring that others can replicate the study, hence this description. The relevance of the study according to Belanger (2012) can be determined by demonstrating that the participants are experts in the field, and therefore, are capable to discuss the topic of concern form a realistic point of view. In this study, participants were computer forensic experts who were well-regarded in their field, and were therefore able to be realistic with their discussions.

4. FINDINGS

All focus group participants were initially asked 'what is organizational forensic readiness' in order to determine their perceptions and views on the area itself. When referring to forensic readiness, the experts identified various attributes such as collection, preservation, preparation and presentation of evidence. Further, an important theme was the need for adequate resources to sustain the forensic readiness program as well as senior management buy-in.

Participants agreed that forensic readiness was essentially "*having their system [the organization] designed in such a way that enables it to get forensics data for you, and the data is preserved, and you can provide data that is probably triangulated with other data, and to be able to prove timeline*" *Expert_1*. Essentially ensuring that "*you have got to store it in a way you could be confident that it has not been manipulated*" *Expert_2*. Other participants suggest that "*it is a holistic approach to the whole topic of having the tools, people, and processes to achieve their goals whether they are from HR perspective or legal perspective*" *Expert_6*. Further, that "*you have got to know what information you have, where it is stored, who is in charge of it, all of that stuff is part of your readiness. But for an organization to be ready you have got to have management buying in, there has got to be a will to be ready, there has got to be recognition that the problem exists*" *Expert_9*.

4.1. Forensic Readiness Capabilities

Participants in the focus groups were asked why they thought an organization might need forensic readiness and what it might be used for. Participants had firm beliefs about how organizations use forensic capabilities. The focus group experts suggested that the concept in the framework of *Forensic Readiness Capabilities* is better conceptualised using the terminology "Objectives". Further, they suggested that organizations might have different objectives, rather than capabilities, which might include the three capabilities suggested by Elyas et al. (2014): legal-evidence management, internal investigations, and regulatory compliance. Additionally, there was strong support for including internal investigations within the legal-evidence management objective as well as other objectives such as "Forensic Response" and "Business Objectives". What was overwhelmingly clear from the participants was that being forensically ready is important for organizations, and organizations have specific objectives when focusing on forensic readiness: "*Having a forensic capability helps organizations to determine what happened, how, and by whom. It also helps organizations to detect and properly respond to incidents*" *Expert_5*.

Impact on DFR Framework: the term *Forensic Readiness Capabilities* will be changed to *Forensic Readiness Objectives*.

4.1.1. Legal-Evidence Management

The main theme coming from many focus group participants was the need to ensure that all forensic evidence must be captured at the highest burden of proof. This is because at the start of an investigation it is frequently unknown what the evidence will be eventually used for. However, some experts were of the opinion that where investigations were not expected to go to court then there was no need to meet an unnecessary high burden of proof.

For example, one participant stated "*your objectives also influence the criteria, because if your criteria is for prosecution you have higher burden of proof, then the amount of proof influences the amount of evidence you have got to gather. If I am just trying to prove that I did not do a mistake, then you don't need to correlate the*

finding to a case" *Expert_1*. Further, "*All forensic investigations should be considered as applicable for court*" *Expert_10*.

Electronic Discovery (or e-discovery) was discussed as a special case. According to Biggs & Vidalis (2009), e-discovery is "*any process in which electronic data is sought, located, secured, with the intent of using it as evidence in a civil or criminal legal case*". One participant pointed out that e-discovery could be improved by forensic readiness, "*Electronic discovery whether it be for legal process, a lot of paperwork now became electronic, so they need to be ready because if they get called up to produce data, they have got to have a record of it and to be able to produce it*" *Expert_4*.

Impact on DFR Framework: E-discovery has been incorporated into the framework as part of the existing category of *Legal-Evidence Management.* Although e-discovery is not explicit in the framework, it is treated as an outcome of being forensically ready and being able to collect legally sound evidence. It is up to the organization how to use the digital evidence: for e-discovery or otherwise.

4.1.2. Regulatory Compliance

Regulatory Compliance was considered to be the most significant forensic objective of organizations primarily because of the need to avoid non-compliance.

Expert_6 argues that organizations ideally develop a forensic capability in response to regulatory discovery orders. They do so to avoid the financial consequences of non-compliance: "*It is typically that an organization that decides to implement some sort of capability generally because they have received a massive discovery order from a regulator and they need to do something, in the first instance. It costs them a lot of money and they have got to do something about it*" *Expert_6.*

Expert_9 listed a number of relevant examples in the US and UK: "*UK bribery act, the US foreign practices act, the United States federal court supreme rules which bills you millions of dollars if you don't have discovery, and Sarbanes-Oxley*". Conversely, organizations may not want any compliance issues and are careful when an incident occurs: "*the word investigation is often dropped from organization's reports to avoid regulatory consequences*" *Expert_4*.

Impact on DFR Framework: due to the importance of *Regulatory Compliance*, we placed it as the first objective in the DFR framework.

4.1.3. Forensic Response & Internal Investigations

Another forensic readiness objective is to investigate organizational incidents such as those related to security.

Expert_5 suggests that: "*you have got to be able to know if one is happening, and how to respond appropriately, and to figure out how did it start in the first place… you get people who hack into your system and you want to figure out who they did it*". However, forensic investigations can be conducted into any incident, as *Expert_3* points out: "*an example is, the things that we are investigating, there is no crime, there is no fraud, it is just an error, and if I can find the error, and if I can find where it happened, then that's my objective*".

Impact on DFR Framework: the objective of *Internal Investigations* has been extended into a more inclusive category termed as *Forensic Response*. *Forensic Response* to incidents may range from simply knowing what had happened, to conducting comprehensive internal investigations.

4.1.4. Business Objectives

A number of secondary objectives were mentioned in the discussion of forensic readiness. These include support for information security objectives, prosecution of employees, reputation, and recovery of lost assets.

Expert_6 noted "*what we have seen is once the forensic capability is put in place, the use almost grows organically: e.g. penetration testing, and assessing all system services for customer's data*". Further, senior executives may be driven to adopt forensic readiness for retribution reasons: "*satisfaction for the directors because they are upset, this person has betrayed their trust and stolen from them, and they would like to recover loss*" *Expert_9*. *Expert_5* suggested that one of the objectives is to ensure your company's reputation in the event of an incident occurring: "*so for instance, if a customer's data is stolen, then you want to assure that some appropriate response will happen*". Finally some participants thought a driving force behind being forensically ready is the ability to recover assets, or avoiding financial loss.

Impact on DFR Framework: a new objective called *Business Objectives* was added to the DFR framework.

4.2. Forensic Factors

Participants in the focus groups were invited to comment on the forensic readiness part of the DFR framework. Overall, the participants made positive comments about the framework with some criticism related to *Training*, *Policy* and *Stakeholders*. Also there was some discussion as to whether *Monitoring* was a DFR factor. Additionally comments were made about whether the left side of the framework should be called *Forensic Factors*, with participants suggesting that these things were in fact the capability. As such, the term *Forensic Readiness Capability* is used to describe the forensic readiness components in the left side of the framework.

Impact on DFR Framework: the term *Forensic Factors* will be changed to *Forensic Readiness Capability*.

4.2.1. Organizational Factors

Participants considered *Top Management Support*, *Governance*, and *Culture* to be implicitly a function of the organization as a whole. Essentially participants thought that these three factors form the basis on which the *Forensic Strategy* can be developed. "*Top Management, Governance, Culture must be interlinked*" *Expert_9*. As such, these factors have been grouped as *Organizational Factors* in the revised DFR framework, and the relationships between them are now shown as implicit, as part of routine organizational processes, rather than explicit as part of the DFR framework.

Impact on DFR Framework: *Top Management Support*, *Governance*, and *Culture* are encapsulated within *Organizational Factors*.

Top Management Support

Across the focus groups there is agreement that senior management support, in terms of funding, staff allocation and political backing, is required for any forensic readiness initiative to be successful.

Regarding management support, one participant said "*absolutely they [senior management] play a role, they are the ones who back it, they are the ones who supporting it*" *Expert_1*. This perspective is shared by *Expert_4* who states that without *Top Management Support* "*it would be extremely difficult to ensure continued funding and staff allocation*". *Expert_2* shares a similar opinion, and argues that the senior management would have genuine interest in supporting the forensic program, as they will be held accountable if an incident occurs and their organization is unable to respond: "*adopting readiness is an easy decision to be made by a senior management, because they are the ones who are directly influenced*".

Overall participants agreed that "*top management drive the organization, support necessary training, and agree to right resources*" *Expert_8* and that "*these people [top management] set the tone. If people below do not see value in a thing in management's view, they will direct resources elsewhere*" *Expert_7*. In fact, several participants were of the opinion that "*top management support, culture, and governance are connected*" *Expert_9*.

Impact on DFR Framework: *Top Management Support* is encapsulated within *Organizational Factors*.

Governance

Forensic governance can be seen from two perspectives. Firstly, governance that is practiced to ensure the efficiency of the forensic program, and secondly, demonstrating good corporate governance by being forensically ready.

Governance here refers to the first category 'governance to ensure the efficiency of the forensic program' as described by *Expert_3*: "*I would want to know whether or not the technology, monitoring system, and architecture have been validated*". *Expert_9* highlights the importance of accountability when implementing a forensic program: "*they also need to have regulated compliance incorporated into the process, so if you don't comply with the forensic readiness model that is in place, there is a penalty for that, because if there is no penalty, people are not going to comply*". As mentioned earlier *Governance*, *Culture* and *Top Management Support* are interlinked implicitly within organizational processes.

Impact on DFR Framework: *Governance* is encapsulated within *Organizational Factors*.

Culture

A forensic *Culture*, for many of the focus group participants, was important to instil in an organization. *Culture* was widely perceived to be driven by top management. The participants discussed the extent to which *Culture* was influenced proactively through education or reactively as a result of experiences.

The predominant perspective on forensic *Culture* was that it had to be driven by top management: "*Culture must be implemented and driven from the top management*" *Expert_9* and "*top management defines the tone of the company. They create the culture and inspire changes to it*" *Expert_7*.

Expert_2 advises to create culture proactively by educating staff about forensics, and not to wait until major incidents occur to start learning. However, they anticipate that forensic awareness will be injected into most organizations after being victims of major incidents: "*get natural injection awareness, you don't want awareness to come about with preference to incidents with respond to incidents, that's not the ideal way, but this is the way lots of organizations are going to inject their awareness*" *Expert_2*.

However there is a belief that because digital forensics is a relatively immature field that as the maturity of the field improves as would an organizational culture that supports forensics: "*The culture of the organization will need to grow / change / accept this idea / concept so that it can be achievable*" *Expert_4*. There are also comments made by participants regarding the nature of culture and forensics with participant *Expert_6* relating "*the use of these [forensic] capabilities is often a cultural change*". This relates to the power that being aware of what is actually going on with the organizations systems has on changing employee behaviour.

Impact on DFR Framework: *Culture* is encapsulated within *Organizational Factors*.

4.2.2. Forensic Strategy

Forensic Strategy is seen as critical for forensic readiness and also unique to each organization. Participants point out that *Strategy* must be designed according to the organization's objectives. Participants brought up a variety of issues related to *Strategy* such as resourcing, planning and risk management.

Expert_6 states that a *Forensic Strategy* is the "*key to success. Management must ensure that there is a robust strategy*". Participants had some overall comments about the *Forensic Strategy* in terms of its purpose. *Expert_9* emphasizes that the *Forensic Strategy* should be designed in accordance with the objectives to be achieved: "*you need to have a forensic strategy, but you need to clearly define the purpose and level of forensic readiness to be achieved*" *Expert_9*. The idea is reiterated by *Expert_10*: "*You should decide about the purpose of the strategy, is it to prosecute? is it a compliance requirement? legal requirement? or contract requirement?*" *Expert_10*. This reinforces the idea that the *Forensic Strategy* is unique to the circumstances of the organization and its forensic objectives.

Impact on DFR Framework: *Forensic Strategy* remains as an encapsulation of the other forensic readiness factors, indicating that the strategy defines the purpose and scope of forensic readiness.

4.2.3. Stakeholders

In the focus groups there was a large evolving discussion on the perceived overlap between *Technical Stakeholders* and *Non-Technical Stakeholders*, and whether the framework was actually discussing *Forensic Stakeholders* and *Non-Forensic Stakeholders* instead. Subsequently, it was realized that stakeholders may be better represented by dynamic roles that may change throughout the lifecycle of the forensic program. For example, a system administrator is considered a *Forensic Stakeholder* while they are cooperating with the forensics team during an incident, but is considered a *Non-Forensic Stakeholder* otherwise. Any other individual or party whether technical, non-technical, internal, or external to the organization is considered a *Forensic Stakeholder* when they are involved in the forensic program, and are *Non-Forensic Stakeholders* at all other times when they are involved with the organization. In other words, *Forensic Stakeholders* are now seen as roles that are filled when necessary as opposed to being permanent positions.

Focus group participants suggested many stakeholders play roles as *Forensic Stakeholders* and *Non-Forensic Stakeholders*. *Forensic Stakeholders* included: IT and security people (*Expert_1*), internal groups, risk groups, human resources (*Expert_2*, *Expert_9*), the CEO, CIO, CTO, & CFO (*Expert_9*) and Accountants (*Expert_3*) when they were undertaking forensic activities. *Expert_9* defines a *Forensic Stakeholder* role as "*someone who has an interest in the forensic side of the application*". *Non-Forensic Stakeholders* were considered by most to be the rest of the organization who were not performing forensic roles: "*pretty much, all the staff is going to need to be involved at some point*" *Expert_1*. Additionally, participants suggested a range of external stakeholders that would be considered either *Forensic Stakeholders* or *Non-Forensic Stakeholders* depending on the role they play in the investigation. These included: Law Enforcement, including police, and lawyers (*Expert_1*, *Expert_2*), an external response team including security experts and forensic experts (*Expert_2*, *Expert_9*) and regulatory bodies (*Expert_3*)

Impact on DFR Framework: the *Technical Stakeholders* and *Non-Technical Stakeholders* are renamed *Forensic Stakeholders* and *Non-Forensic Stakeholders* within which, stakeholders of each type could be internal or external to the organization.

4.2.4. Forensic Infrastructure

The participants considered the combination of three factors, i.e. *Monitoring*, *Architecture* and *Technology*, to be the driving force behind a forensics capability.

Additionally, *Technology* and *Architecture* (see section on *Monitoring* as to why this isn't included) seemed to be inherently related: "*The technology can be in place but will not be effective without the correct architecture*" *Expert_6*. Additionally, *Expert_7* points out that "*the level of available technology (including existing systems) will decide what the architecture can do, but the architecture can influence technology buying / decommissioning also*". As such, the framework was changed to include a *Forensic Infrastructure* box in which *Architecture* and *Technology* are included, and have implicit relationships around the design of the architecture given the technology.

Impact on DFR Framework: *Architecture* and *Technology* are encapsulated within *Forensic Infrastructure* which implies an implicit two way relationship between these two factors.

4.2.5. Monitoring

All participants agree that actively monitoring the system in order to promptly detect incidents is crucial for forensics. However, whether *Monitoring* can be part of an organizational forensic framework is debatable. *Monitoring* is largely perceived as a security function. *Expert_8* seemed reluctant to accept that *Monitoring* is a forensic function, however acknowledged its importance: "*I had a Yes/No for system monitoring. Because forensics is a lot more reactive, rather than actively monitoring, but certainly it does help*". *Expert_4* holds similar opinion: "*I agree 100%, but I thought it comes with security, security software will most likely identify anomaly, and that would trigger a forensic response*".

Due to its grounding in security, *Monitoring* has been dropped from the forensics framework as a major factor. However, the *Monitoring* function is diffused throughout the framework. *Monitoring* is part of the forensic *Architecture* that is designed to detect incidents and maintain the integrity of evidence. *Monitoring* tools are part of the forensic *Technology*. What is to be monitored is planned for in the *Forensic Strategy*, documented in the *Forensic Policy*, and prepared for through *Forensic Training*. *Forensic Stakeholders* include system administrators and security officers who monitor the system, and report to the forensics team when necessary. Monitoring is also influenced by the *Organizational Factors*.

Impact on DFR Framework: *Monitoring* has been removed from the DFR framework.

4.2.6. Architecture

The participants thought that a key factor that influenced forensic readiness was the extent to which the design and configuration of the IT architecture complemented the forensic process.

Expert_3 states "*the IT systems should be designed in such a way that information is continuously recorded and prevented from being tampered with*". *Expert_7* suggests further, "*when designing a forensic system, you have got to figure out how it fits to the existing systems in the organization*". *Expert_6* agrees with this assessment stating "*the technology can be in place but will not be effective without the correct architecture*" and further suggests that the *Architecture* will change as technology changes. An example of a forensically designed system is a system where "*logs, CCTVs, and systems that identify who was at particular computer at particular time, are all installed. Also you may need to store all these logs in one place, and making them easy to read*" *Expert_1*. The forensic design of a system may require the deployment of extra artefacts, or reconfiguring the existing artefacts with forensics in mind: "*You can deploy monitoring system, you can use existing systems you have got in place, but you will need to increase the purposiveness of what you are logging, increase the retention of what you log*" *Expert*_3. *Expert_1* argues that most computing systems by default are configured to collect information: "*in the ideal word, all computer systems record just enough information to solve whatever crime or event or thing that I am investigating… these artefacts are not there for forensic purposes, they are there to solve user's convenience issues*". An example is internet cookies that are produced by the browser to accelerate access to websites previously visited. Another example is internet history which is designed to be used as a reference for users. These artefacts could be rich sources of information for forensic investigations. Overall there is agreement that *Architecture* is an important factor in forensic readiness.

Impact on DFR Framework: *Architecture* is included within *Forensic Infrastructure*.

4.2.7. Technology

The *Technology* factor represents the technologies used in the organization: both in its normal operations, and that technology which is specifically used for forensic purposes. Participants did not overly concern themselves

with the technologies used for everyday business operations, other than to state that they should have logging features enabled and be architected in a way that is useful for forensics.

There were many comments about the need to ensure that *forensic technology* was present to enable forensic tasks. "*In order to perform the forensic tasks, the organization will need to utilize a forensic toolkit*" *Expert_2*. Participants were of the opinion that due to the strict court requirements with regard to technologies used to examine digital evidence, such technologies must be "*validated through either industry certification, expert testimony, or having the vendor testifying that the technology works, and that the organization used it the right way*" *Expert_1*. As such, participants were of the opinion that "*forensic technologies are highly specialized, they need practice and experience*" *Expert_5*. In addition to having the appropriate hardware and software available to do the job, participants were quick to warn that "*keeping [the] technology up to date and using what is needed to achieve the forensic objectives is critical to any effort*" *Expert_7*. They were also quick to point out that cost is an issue for the organization. Finally, participants warned that just having the technology might not be enough: "*but you can't rely completely on technology. [It] does not replace well-trained staff and good procedures*" *Expert_11*.

Impact on DFR Framework: *Technology* is encapsulated within *Forensic Infrastructure*.

4.2.8. Forensic Policy

The *Forensic Policy* is the compulsory formalisation of the rules that address the people, process and technology of the organization has with regards to forensics. It should be sponsored by senior management, authored by forensic and/or non-forensic stakeholders and could be incorporated into the organizational policy suite or could be an independent policy.

Participants were clear that *Forensic Policy* is a compulsory requirement of forensic readiness: "*organizations need forensic policies*" *Expert_3* as a *Forensic Policy* "*helps to achieve the [forensic] strategy*" *Expert_8*. *Expert_3* states that "*a forensic policy should cover the areas of people, process, and technology. It should also cover the areas of OS, network, and application forensics*". This is agreed with by other participants. *Expert_5* takes this further by stating the role of policy: "*the role of the policy is to determine, well the word procedure is coming, often procedures go with policies, it is a sort of regulation or how we do things, it is a rulebook, it is what you have to do around a certain topic*". This implies that policy is a set of rules that are meant to guide people on what is or is not appropriate with regard to a certain topic – in this case, forensic readiness. *Expert_9* emphasises that the *Forensic Policy* must be driven by and sponsored by senior management: "*you have got to have a management policy, a policy that is driven by top management, it is enforced, it is trained on, regularly reviewed, and tested*".

A *Forensic Policy* could be an independent document apart from other organizational policies, or could become part of other policies (such as the security policy or incident response policy) of the organization. *Expert_1* believes that "*it would be more appropriate for a forensic policy to be part of other policies*". *Expert_3* agrees: "*the policy has to be integral to whatever you are doing*". Subsequently, participants suggested that employees must be made aware of their policy compliance requirements: "*It should be made clear for employees what is appropriate and what is not. Also the consequences of non-compliance should be made clear*" *Expert_10*. If employees are not educated about the policy, this may be taken as an excuse should the policy be violated: "*when the company tries to prosecute 'Bob' who accessed materials that he shouldn't, 'Bob' would argue: a) nobody told me not to do so and b) other people are doing it too*" *Expert_9*.

Impact on DFR Framework: *Policy* has been renamed *Forensic Policy* in the DFR framework.

4.2.9. Forensic Training

The participants suggested that *Forensic Training* can be conceived in two ways. Firstly, *Forensic Training* for *Forensic Stakeholders* in how to conduct forensic investigations, how to use forensic tools etc., and secondly, *Forensic Training* for *Non-Forensic Stakeholders* about the *Forensic Policy* and how to recognise and respond to an incident. The Forensic Stakeholder requires training in the tools and techniques specific to forensic investigation whereas from the perspective of the non-Forensic stakeholder, training is required for basic awareness, evidence preservation, and execution of forensic processes and procedures.

On the types of training, the participants noted that "*There will be different sets of training based on the audience*" *Expert_2*. "*The forensics team needs to attend technical training, while the [general] staff needs only to be trained on data preservation*" *Expert_4*. Each of these training types must be designed and delivered to the appropriate stakeholders. "*The forensics team may need professional training and the normal users should only know how to contain an incident, so not to do anything technical, but to know how to preserve the evidence*" *Expert_4*.

From a *Forensic Stakeholder's* perspective, *Forensic Training* is important to have on the tools and techniques of forensic investigation. "*If you have got to do anything you have got to have qualified people to do it, if you do not have qualified people you cannot present evidence in court*" *Expert_4*. Without adequate *Forensic Training* for the *Forensic Stakeholders* the level of forensic readiness will be affected. From a *Non-Forensic Stakeholder's* perspective, *Forensic Training* is conducted around awareness: "*<staff> are going to need to know what the processes are if things happen*" *Expert_1*. Additionally, *Non-Forensic Stakeholders* will need to be able to identify when an incident has occurred so that they can begin to implement the *Forensic Policy* processes.

Expert_3 argues that *Forensic Training* will not only educate staff about their forensic duties, but will also let them appreciate the value of being forensically ready: "*training helps people to understand and appreciate the process. When they know that the process is for their benefit (e.g. providing evidence of their innocence), they are more likely to appreciate readiness*" *Expert_3*.

Impact on DFR Framework: *Training* has been renamed *Forensic Training* in the DFR framework and the definition and description changed to explain the different types of training encapsulated by the *Forensic Training* factor.

4.3. Relationships Between Factors

As part of the second and third focus groups, participants were asked to identify relationships between the forensic readiness factors and to comment on these relationships. Two identical lists of DFR factors were given to the participants. The participants were asked to identify the top eight relationships in terms of significance by drawing arrows between the two lists and adding comments. No significant relationships other than those in (Elyas et al. 2014) (see Figure 1) were identified. However, the participants suggested that there was a strong correlation between Forensic Technology and Forensic Architecture, and therefore, these were grouped together in one box labelled as 'Forensic Infrastructure'. The participants also suggested that Forensic Culture, Top Management Support, and Forensic Governance are closely connected, and therefore, these were grouped together in one box labelled as 'Organizational Factors'. Further, the participants were explicitly asked to express their agreement / disagreement with the relationships proposed in this research (see Figure 1). The participants unanimously agreed with the proposed relationships.

The validated DFR relationships are discussed in this section with full descriptions provided in Appendix 4. In the headings in the next sections, the relationships are named R1...R8 as they appear in Figure 2. Numbers in brackets are the relationships as they appeared originally in Figure 1.

4.3.1. R1 (C1) –Forensic Readiness Capability and Forensic Readiness Objectives

There was general agreement from participants that the relationship, *R1*, between *Forensic Readiness Objectives* and *Forensic Readiness Capability* exists and is bi-directional. In Elyas et al. (2014)'s original DFR framework there was a concern that investigations would be treated differently because the factors *Legal-Evidence Management* and *Internal Investigations* were separate. However, when commenting on the relationship *R1*, participants pointed out that you have to investigate in the same way regardless.: "*Treat all investigations as if it will go to court. Sometimes you simply do not know what / when / how the evidence collected will be used, eg. a small investigation may lead to a lawsuit*" *Expert_8*. The bi-directional nature of the relationship is captured by members of focus group 1 who point out: "*I suppose there would be a link both ways, to meet the objectives you have got to have a strategy*" *Expert_1*. *Expert_2* suggests that the relationship also needs to capture the: "*need to have the objectives before you know what your strategy is*".

4.3.2. R2 (O1, O2 &O3) – Organizational Factors and Forensic Strategy

The participants linked all three of the organizational factors to the *Forensic Strategy* and its components. Top management plays a critical role in supporting strategy by providing resources and moral support to stakeholders. Further, participants pointed out the key role of governance and organizational culture in the success of strategy as well as other capability factors.

From a *Top Management Support* perspective, *Expert_4* asserts "*without the support of management, the forensic strategy is unlikely to succeed*". This is seconded by *Expert_6* who states: "*Key to success! Management must ensure that there is a robust strategy*". *Expert_4* stated that the top management should give stakeholders the sense of ownership of forensics, in order for the program to succeed, while *Expert_6* believes that the main role of the senior management is to allocate resources: "*It is crucial that management assign the right amount of resources*". The *Governance* perspective is supported by *Expert_8* who believes that *Governance* is key to achieving the strategy, while *Expert_6* suggests that the "*organizational culture must be supportive of forensics in order for the strategy to succeed*".

Further support for this relationship is provided between *Organizational Factors* and various *Forensic Strategy* components. *Expert_7* says to never underestimate the value that management plays in *Forensic Training*: "*top management should drive the importance of training or people may not take it seriously*". *Governance* plays a role in ensuring that the right *Forensic Training* is delivered: "*understanding / identify the right processes and procedures, assist the identification of necessary training required for company employees*" *Expert_8*. *Governance* also ensures that the *Forensic Policy* is implemented and complied with, and that it is in line with laws and regulations. "*Policies drive what governance looks for or ensures, but governance can find things to change / improve the policies*". *Expert_6* asserts that *Governance* is also important for transparency reasons: "*A robust governance system is critical to ensure system is transparent*". The organizational culture must change and support forensics in order for the objectives of the *Forensic Strategy* to be achieved: "*The culture of the organization will need to grow / change / accept this idea / concept [forensic readiness] so that it can be achievable*" *Expert_4*. *Expert_8* believes that *Culture* is driven by the *Forensic Stakeholders* and top management: "*stakeholders drive the culture, as do top management*".

4.3.3. R3 (S2) – Forensic Stakeholders and Forensic Policy

The relationship, *R3*, between *Forensic Stakeholders* and *Forensic Policy* reflects the involvement of *Forensic Stakeholders* in writing the *Forensic Policy* (along with *Non-Forensic Stakeholders*) and their being subject to the actions specified in the policy. *Expert_6* asserts that "*it is critical that the [forensic] stakeholders comply with the workable policy*". Additionally *Expert_7* reiterates the importance about including *Forensic Stakeholders* in the development process "*As staff who understand the scope and difficulty of the forensic efforts, the tech [forensic] group should work closely with the policy makers*".

4.3.4. R4 (S5) – Forensic Stakeholders and Forensic Training

The role of *Forensic Stakeholders* in *Forensic Training* is two-fold. Firstly, *Forensic Stakeholders* will be involved with the development of *Forensic Training* for *Non-Forensic Stakeholders*, and may also be involved in the development of *Forensic Training* for other members of the forensics team. *Expert_7* suggests that "*stakeholders should help form the training that is relevant to what they do*".

Secondly, *Forensic Stakeholders* must undergo *Forensic Training* so that they are kept up to date with forensic software tools and forensic techniques. *Expert_4* suggests that the *Forensic Training* for *Forensic Stakeholders* may be sourced externally: "*[the] forensics team will need to attend technical training – it should be outsourced in most instances unless you have written the software / coding etc.*" *Expert_4*. Additionally, *Expert_7* suggests that the *Forensic Stakeholders* "*can learn relevant new procedures and methods from it [training], as well as updates*".

4.3.5. R5 (S1) – Non-Forensic Stakeholders and Forensic Policy

The relationship, *R5*, between *Non-Forensic Stakeholders* and *Forensic Policy* reflects the involvement of *Non-Forensic Stakeholders* in writing the *Forensic Policy* (along with *Forensic Stakeholders*) and their being subject to the actions specified in the policy. From a development perspective, participants were clear that involvement of non-forensic stakeholders such as policy writers is critical in the policy development: "*non-technical stakeholders are the ones who develop policies*" *Expert_5*. From the *Forensic Policy* compliance perspective, *Expert_6* emphasizes on the importance of stakeholders' compliance with the policy: "*It is crucial that the stakeholders comply with the workable policy*". *Expert_7* also agrees stating "*Non-technical people especially need the policy to make sure they know what to do, and post learning can influence the policy*".

4.3.6. R6 (S4) – Non-Forensic Stakeholders and Forensic Training

Participants agreed that the relationship R6 is bi-directional as non-forensic stakeholders need to be trained on a range of forensic issues such as data preservation, policy and capability. At the same time non-forensic stakeholders can provide feedback on the effectiveness of the training program.

The relationship *R6* is confirmed by *Expert_2* "*I think training educates stakeholders and stakeholders attend training and that is great*". *Forensic Training* is important and differs for *Non-Forensic Stakeholders* and *Forensic Stakeholders*. *Expert_4* stressed "*the forensics team needs to attend technical training, while the [non-forensic] staff needs only to be trained on data preservation*". The view of *Expert_6* is similar: "*non-technical staff don't need to be trained on forensics, but they need an overarching understanding of the capabilities*". *Expert_7* states that the *Non-Technical Stakeholders* are the most who need the *Forensic Policy* and *Forensic Training*: "*in particular, non-technical staff needs the policy and training to understand the rules*".

4.3.7. R7 (S3) – Non-Forensic Stakeholders and Forensic Stakeholders

The relationship between *Forensic Stakeholders* and *Non-Forensic Stakeholders* represents the two way communication between these groups. This communication is critical for the complete forensics process.

Communication will occur regarding the development and delivery of *Forensic Policy* and *Forensic Training*, as well as in the event of an incident. When discussing the relationship between the sets of stakeholders, *Expert_7* suggested that communication is important as: "*To learn what happened they have to be able to communicate and gather information properly*" *Expert_7*.

4.3.8. R8 (S6, S7 & S8) – Forensic Stakeholders and Forensic Infrastructure

Relationship, *R8*, depicts a one-way relationship indicating the involvement of *Forensic Stakeholders* in the development, maintenance and use of the *Forensic Infrastructure* of the organization. *Expert_7* argues that "*technical stakeholders help shape architecture*" and that they must "*know what to do to respond [to an incident]*". *Expert_10* states that further involvement with *Forensic Stakeholders* and the *Forensic Infrastructure* is with maintenance and testing: "*Consider maintenance of systems and testing of systems*". There are also comments of indirect links made by participants where the *Forensic Stakeholders* are conduits between the *Forensic Infrastructure* and *Forensic Policy*. *Expert_4* also believes that the *Forensic Infrastructure* is indirectly influenced by *Forensic Policy* through *Forensic Stakeholders*. That is, the *Forensic Policy* dictates what level of privacy is expected, what standard is to be used for technologies, and the aspects of the *Forensic Infrastructure*. This is seconded by *Expert_5*, "*policy can have an impact on the architecture of the system*".

4.4. Summary

The framework defined by Elyas et al. (2014) was changed in a number of ways as a result of the validation and refinement exercise undertaken using the focus groups. A summary of these changes are provided in Table 2. Subsequently, Elyas et al.'s DFR framework has been re-specified as shown in Figure 2. Full definitions (and descriptions) for each of the objectives and factors in the framework are presented in Appendix 3, and the descriptions of the relationships between factors are summarized in Appendix 4.

Table 2: Summary of Framework Changes

Area in Elyas et al.'s (2014) Framework	**Change**
Forensic Readiness Capabilities	Changed name to Forensic Readiness Objectives
Legal-Evidence Management	Incorporated Electronic Discovery (still called Legal-Evidence Management)
Internal Investigations	Subsumed within Forensic Response (new category)
Regulatory Compliance	Moved to be the first objective to reflect its perceived importance
[Forensic Response]	New objective suggested by participants
[Business Objectives]	New objective suggested by participants
Forensic Factors	Changed name to *Forensic Readiness Capability*
[Organizational Factors]	*Top Management Support*, *Governance*, and *Culture* are encapsulated within *Organizational Factors*.
Top Management Support	*Top Management Support* is encapsulated within *Organizational Factors*.
Governance	*Governance* is encapsulated within *Organizational Factors*.
Culture	*Culture* is encapsulated within *Organizational Factors*.
Forensic Strategy	*Forensic Strategy* remains as an encapsulation of the other forensic readiness factors, indicating that the strategy defines the purpose and scope of forensic readiness.
Non-Technical Stakeholders	The *Non-Technical Stakeholders* are renamed *Non-Forensic Stakeholders* within which, stakeholders could be internal or external to the organization.
Technical Stakeholders	The *Technical Stakeholders* are renamed *Forensic Stakeholders* within which, stakeholders could be internal or external to the organization.
[Forensic Infrastructure]	New objective: *Architecture* and *Technology* are encapsulated within *Forensic Infrastructure* which implies an implicit two way relationship between these two factors.
Monitoring	*Monitoring* has been removed from the DFR framework
Architecture	*Architecture* is encapsulated within *Forensic Infrastructure*.

Area in Elyas et al.'s (2014) Framework	Change
Technology	*Technology* is encapsulated within *Forensic Infrastructure*.
Policy	*Policy* has been renamed *Forensic Policy* in the DFR framework.
Training	*Training* has been renamed *Forensic Training* in the DFR framework and the definition changed to explain the different types of training encapsulated by the *Forensic Training* factor

The new framework has grouped *Governance*, *Top Management Support* and *Culture* inside *Organizational Factors*. The relationships between these factors are now intrinsic to the operation of the organization and are outside the scope of the framework. Likewise, *Technology* and *Architecture* are grouped within *Forensic Infrastructure* as they are closely related and inter-dependent. This relationship is not shown in the framework due to its intrinsic nature.

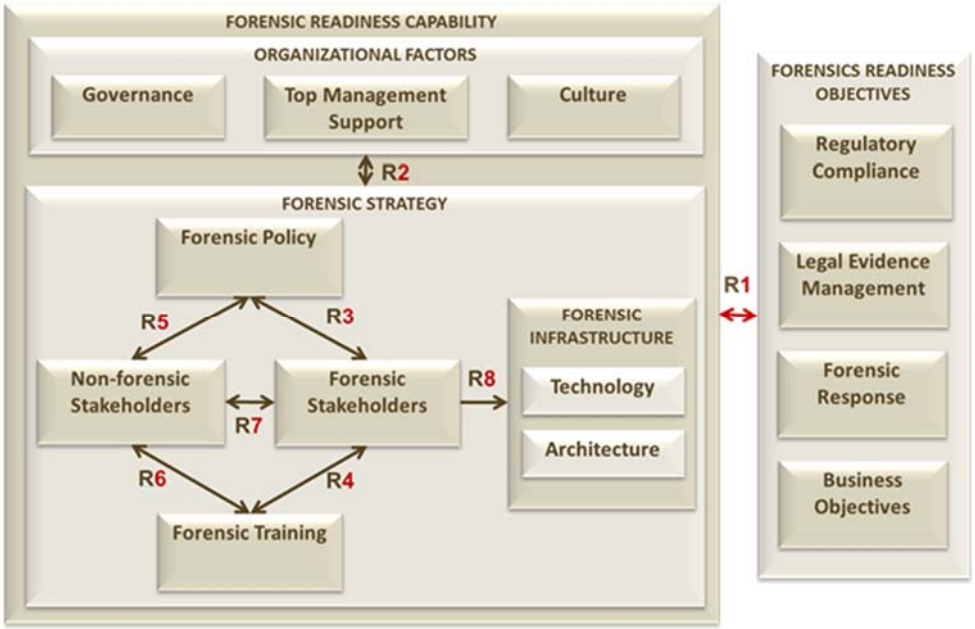

Figure 2: The DFR Framework Resulting from the Focus Group Analysis

5. DISCUSSION: EXPERT PERSPECTIVES

All focus group participants agreed that 'forensic readiness' was an important capability for organizations. Interestingly, although there were four *Forensic Readiness Objectives*, the experts thought that two objectives: 1) the need for organizations to comply with regulations and 2) the need to manage evidence for legal purposes, were most important (as opposed to, for example, conducting internal investigations). This view is likely be rooted in the management culture of Australian organizations where compliance to legal and regulatory agencies is considered extremely important (see discussion on Australian compliance culture in the context of security management in Tan et al, (2010) and Shedden et al., (2010)). The participants also suggested that the role of forensic readiness extends from the narrow function of being able to conduct *Internal Investigations* to the wider context of providing comprehensive *Forensic Response* to incidents.

Adopting a forensic readiness plan is also likely to improve the security posture of the organization. The focus group participants suggest that DFR supports the information security program by enhancing the security posture and deterring potential attackers. Investigation reports can be used to review and assess the current security controls, and subsequently address vulnerabilities. The report may also be used to improve the security strategy and security policy (see Ahmad et al. (2014) for a discussion on security strategy and deterrence). This notion has also been supported by the focus group participants: "*the role of forensics is integrative to security. New ideas about risks and vulnerabilities might emerge as a result of an investigation*" Expert_4. Grobler and Louwrens (2007) suggest that forensic readiness be seen as an information security best practice, as it helps organisations demonstrates that reasonable care has been taken to protect information assets and that security incidents are more likely to be successfully investigated.

Competition among the forensic readiness objectives was a source of much debate. Given it is typically unknown at the start of a forensic investigation how evidence may be used, some experts suggested that all evidence should be collected to satisfy the highest burden of proof. Other experts argued that the cost of compliance with legal standards is high, making it infeasible for universal application to all forensic investigations. The participants agreed that a compromise position might be to take a risk oriented approach and assess the likelihood and impact of various scenarios to assist in decision-making at the start of a forensic investigation. As an aside, there was a related discussion on the decision of senior management to develop a DFR capability. The participants suggested that prior major incidents would likely accelerate the decision to adopt forensic readiness (especially if the incident caused significant financial damage).

Implicit in the discussion of the left hand side of the framework was the view that *Forensic Strategy* is a plan (as opposed to a process, ploy etc.) that is closely tied to the organization's forensic objectives and incorporates all factors except for three (*Top Management Support, Governance and Culture*) as they were considered external to DFR but still internal to the organization.

Another interesting discussion focused on part of organizational culture that relates to DFR. A key question was to what extent forensic culture was an outcome of proactive endeavours such as awareness training or was the result of post-incident experiences (a similar debate occurs in security management, see Lim et al., (2010)). Some participants believed that organizational culture would evolve with the maturity of DFR. A key factor in the evolving culture would be the opportunity to use forensic capabilities in other non-traditional areas such as audit.

The focus groups featured an evolving discussion on how best to represent the various types of stakeholders in DFR and their relationships with other factors. The participants agreed that the two sets of stakeholders (*Forensic Stakeholders and Non-Forensic Stakeholders*) would be better represented by dynamic roles that may change throughout the lifecycle of the forensic program. These two types of stakeholders interact differently with the other components of the framework. For example, while *Forensic Stakeholders* have to attend in-depth *Forensic Training*, basic awareness *Forensic Training* may be more appropriate for *Non-Forensic Stakeholders*. The awareness training itself may be delivered by the *Forensic Stakeholders*. On the other hand *Non-Forensic Stakeholders* contribute to the training program through their feedback. The interaction of the different stakeholders with the *Forensic Policy* is also different. The *Forensic Policy* may be developed by the *Forensic Stakeholders*. However, the policy will be improved through the feedback of the *Non-Forensic Stakeholders*. Once the policy is enforced, all stakeholders – forensic and non-forensic – are expected to comply.

The role of external stakeholders was another key discussion point especially since many of the participants were consultants and were frequently playing that role. On the one hand external stakeholders were not being trained, using the technology to meet organizational objectives, but they were required to comply with organizational policies when they were members of the organizational DFR team.

The closely coupled relationship between *Technology* and *Architecture* was widely acknowledged however the participants debated whether *Monitoring* of incidents that trigger forensic investigations was a security function rather than a forensic one. Conceptual distinctions aside, the participants debated the extent to which systems had to be specifically engineered for evidence collection. The term 'purposiveness' was used to capture the need for systems configuration to reflect the intent to collect evidence of a particular kind.

A number of themes cut across the discussion of factors. For example, participants discussed the implications of cloud-based resources on forensic investigations. One participant stated "*Forensic utopia died about five years ago, as soon as companies started pushing data into the cloud*" (*Expert_9*). The experts commented that the complexity of corporate investigations is increasing every day, cloud computing in particular raises serious challenges for traditional investigative methodologies. The corporate data is stored somewhere in the cloud, and the investigators have little control over who can access the data while investigations being held, which raises issues about the integrity of data. Another point of discussion was the influence of organizational size on each of the factors. For SMEs with a single systems administrator responsible for IT, all of the forensic roles and the functions in the framework would have to be implemented by a single person which raises the issue of what trade-offs exist for organizations resourcing proactive forensic readiness.

6. USING FOCUS GROUPS IN THIS STUDY

By reviewing articles published in forensic readiness, it can be noted that propositions in this area are generally characterized by: a) conceptual development, and b) lack of validation. This comes as no surprise as the field of digital forensics is generally practice-driven. However there have been numerous calls by prominent researchers to increase the level of rigor in digital forensics research. For example, Beebe (2009) suggests that digital forensics can only progress as a scientific discipline if the methodological rigor of studies is raised. Our review

shows that most propositions in forensic readiness are conceptually developed with little or no validation. Conceptual studies refer to research that is not supported by empirical data and that is largely based on the researcher's creative endeavour or experience (Poeppelbuss, Niehaves, Simons et al., 2011). Validation is "the process of ensuring that the model is sufficiently accurate for the purpose at hand" (Beecham, Hall, Britton et al., 2005) – the purpose being forensic readiness in this case.

A systematic literature review (Okoli & Schabram, 2010) and knowledge synthesis approach using coding techniques as described in Grounded Theory (see Strauss & Corbin, 1994; Wolfswinkel, Furtmueller, & Wilderom, 2011) have been utilised in this study to define a more holistic understanding of forensic readiness, which was subsequently developed into a new model. As shown in this paper, the new model has been validated through three independent focus group studies of computer forensic experts. The focus group method allows the researchers to collect rich and diverse data in a relatively short time, and it encourages the participants to discuss issues of significance and reflect on each other's views (Kitzinger, 1995). The participants of the focus groups were well-experienced and authoritative, with digital forensics work experience that spans across various organizations and different industries. This enabled the researchers to acquire rich information for the purpose of model refinement and validation. Furthermore, adopting a multi-focus group design allowed the researchers to triangulate the results of the individual studies. The use of focus groups is therefore a strength of this study and it contributes to an increased rigor of research in the area. Although this is a considerable step forward, this can be further improved by using a larger sample of computer forensic experts in the form of a Delphi study – which the researchers intend to do in future.

7. CONCLUSION & FUTURE WORK

A major contribution of this study is the introduction of a new model that can be used by organisations to assess their forensic readiness. The model has discriminating power that enables organisations to assess their forensic strategy. This power is provided by the identified factors, relationships and definitions that can collectively be used as an instrument to assess forensic readiness. For example, to assess the utility of forensic strategy, the framework suggests the following must exist: leadership commitment towards forensics, staff awareness and commitment towards forensics, organisational structure that takes forensics into consideration, enforcement of forensic policy and training, accountability of staff towards their forensic responsibilities, active monitoring and continuous assessment of system activities.

The proposed framework can also be used by organisations with no forensic plans to inform the development of a forensic capability. The objectives of the model help decision makers understand what to expect out of the forensic capability. The proposed forensic readiness factors help organisations understand what needs to be critically considered when developing the capability. Finally, the relationships of the model will explain how the factors interact to achieve the state of forensic readiness in the organisation. This is another significant practical contribution of the study considering the lack of guides and standards with respect to forensic readiness. Further, the proposed framework can be formalised and transformed into an industrial guide for forensic readiness.

The framework also shows that forensic readiness primarily helps organisations to comply with regulations, properly manage digital evidence, and forensically respond to incidents, in addition to other non-forensic objectives. The identification of a limited and well-established set of objectives, will help decision makers understand how their organisations benefit from forensic readiness. Furthermore, recognition of non-forensic objectives in the model highlights the business potential of implementing a forensic plan, which may – for some organisations – provide the needed justification to invest in forensic readiness.

This research also suggests that organisations of all sizes may develop a forensic capability. While all factors introduced in the proposed model will need to be considered, the way these are implemented will differ from one organisation to another. For example, organisations may hire new staff, training existing staff, or contract with external parties to carry out the forensic tasks, according to their special circumstances. Whatever option the organisation selects, it will represent the *Forensic Stakeholders* component of the model. In other words, the size of the organisation and limited resources are NOT excuses for not being forensically ready. The flexibility offered by the model is likely to encourage a larger organisational sector to adopt forensic readiness.

The focus group experts suggested that organisational IT security can greatly benefit from having a forensic capability. Organisations may take advantage of the forensic investigative reports to review and improve their security strategy. The ability to investigate incidents using in-house resources will enable organisations to identify system vulnerabilities and subsequently strengthening their defences. Furthermore, when the organisation is known to implement a forensic plan, this may serve as a further deterrent for future intruders. Organisations that implement forensic plans are more likely to be successful on tracing culprits and producing incriminating evidence. Establishing the relationship between forensic readiness and IT security is an important

contribution. For organisations that are security focused, this may provide stronger justification to invest on forensic readiness.

One of the key contributions of this study is that stakeholders in the forensic program cannot be treated as one entity. The study reveals that organisations have to deal with two distinct groups of stakeholders, forensic and non-forensic. Forensic stakeholders take the lead by being directly responsible for training, policy, and other key aspects of the forensic program. On the other hand, non-forensic stakeholders are required to develop basic forensic awareness, so that they learn how to behave in a way that does not compromise the integrity of potential digital evidence. The engagement of non-forensic stakeholders in forensic training and policy is important as the first responder to an incident can be anyone in the organisation. It is hoped that this research will draw attention to the important role played by those not directly involved in the forensic program 'non-forensic stakeholders'. One implication of this is that forensic training and policy will no longer be exclusive to those directly involved in the forensic program. All staff will be required to attend forensic awareness training and comply with forensic policy.

The focus group study discussed in this paper provides rich insights with respect to what the experts thought of the proposed framework. The framework will undergo further validation in future research through a multi-round Delphi survey. The purpose of the Delphi study is to triangulate the outcomes of the focus groups and to gain quantified consensus with respect to the components of the forensic readiness framework (i.e. objectives, factors, and relationships). The Delphi study will be conducted with a particular focus on the definitions and descriptions of the framework's components.

8. ACKNOWLEDGEMENTS

We are sincerely grateful to all the experts who participated in this study. The write-up of this manuscript has been supported by Albert Shimmins Postgraduate Writing-up Award.

9. REFERENCES

Ahmad, A., Maynard, S. B., & Park, S. (2014). Information security strategies: towards an organizational multi-strategy perspective. Journal of Intelligent Manufacturing, 25(2), 357-370.

AIC. (2009). The Australian Business Assessment of Computer User Security: A National Survey. Australia: Australian Institute of Criminology.

AusCert. (2006). Computer Crime and Security Survey. Australia.

Beebe, N. (2009). Digital Forensic Research: The Good, The Bad, and The Unaddressed *Advances in Digital Forensics V* (pp. 17-36). US: International Federation for Information Processing.

Beecham, S., Hall, T., Britton, C., Cottee, M., & Rainer, A. (2005). Using an expert panel to validate a requirements process improvement model. *Journal of Systems and Software, 76*(3), 251-275.

Belanger, F. (2012). Theorizing In Information Systems Research Using Focus Groups. *Australasian Journal of Information Systems*, 109-135.

Biggs, S., & Vidalis, S. (2009). *Cloud computing: The impact on digital forensic investigations.* Paper presented at the Internet Technology and Secured Transactions, 2009. ICITST 2009. International Conference for.

Carrier, B., & Spafford, E. H. (2003). Getting physical with the digital investigation process. *International Journal of digital evidence, 2*(2), 1-20.

Casey, E. (2005). Case Study: Network intrusion investigation - lessons in forensic preparation. *Digital Investigation*, 254-260.

Elo, S., & Kyngäs, H. (2008). The Qualitative Content Analysis Process. *Journal of Advanced Nursing*, 107-115.

Elyas, M., Ahmad, A., Maynard, S., & Lonie, A. (2014). Forensic Readiness: Is Your Organisation Ready? *Digital Forensic Magazine*, 58-62.

Ghosh, A. (2004). *Guidelines for the Management of IT Evidence.* Paper presented at the APEC Telecommunications and Information Working Group, China.

Grobler, C., & Louwrens, C. (2007). *Digital forensic readiness as a component of information security best practice.* Paper presented at the 22nd International Information Security Conference, Sandton, SOUTH AFRICA.

Grobler, C., Louwrens, C., & von Solms, S. (2010). *A framework to guide the implementation of Proactive Digital Forensics in organizations.* Paper presented at the International Conference on Availability, Reliability and Security.

ISO17799. (2006). AS/NZS ISO/IEC 17799:2006. Australia/New Zealand: Standards Australia - Standards.

Kitzinger, J. (1995). Qualitative Research: Introducing Focus Groups. *BMJ*, 299-302.

Krueger, R. A., & Casey, M. A. (2001). Designing and conducting focus group interviews. *Social Analysis Selected Tools and Techniques*, 4-23.

Lim, M., Ahmad, A., Shanton, C., Maynard, S. 2010. Embedding Information Security Culture: Emerging Concerns and Challenges. Proceedings of the Pacific Asia Conference on Information Systems (PACIS). Taipei, Taiwan. July 9-12, 2010.

Marcella Jr., A. J. (2008). Electronically stored information and cyberforensics. *Information Systems Control Journal*, 44-48.

Morgan, D. L. (1996). Focus Groups. *Annual Review of Sociology*, 129-152.

Mouhtaropoulos, A., Li, C.-T., & Grobler, M. (2014). Digital Forensic Readiness: Are We There Yet? *Journal of International Commercial Law and Technology, 9*(3), 173-179.

NIST. (2006). Guide to Integrating Forensic Techniques into Incident Response. US: NIST SP800-86 Notes.

Okoli, C., & Schabram, K. (2010). A Guide to Conducting a Systematic Literature Review of Information Systems Research. *prouts: Working Papers on Information Systems*.

Pangalos, G., Ilioudis, C., & Pagkalos, I. (2010). *The importance of Corporate Forensic Readiness in the information security framework.* Paper presented at the 2010 Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises, Larissa.

Pangalos, G., & Katos, V. (2010). Information Assurance and Forensic Readiness. *e-Democracy*, 181-188.

Poeppelbuss, J., Niehaves, B., Simons, A., & Becker, J. (2011). Maturity models in information systems research: literature search and analysis. *Communications of the Association for Information Systems, 29*(27), 505-532.

Pollitt, M. (2010). A History of Digital Forensics *Advances in Digital ForensicsVI* (pp. 3-15). Hong Kong, China: International Federation for Information Processing.

Reddy, K., & Venter, H. (2013). The architecture of a digital forensic readiness management system. *Computers & security, 32*, 73-89.

Reyes, A., & Wiles, J. (2007). Developing an Enterprise Digital Investigative/Electronic Discovery Capability *The Best Damn Cybercrime and Digital Forensics Book Period* (pp. 83-114). US: Syngress.

Richardson, S. (2005). Compliance and Computer Forensics. US: Technology Pathways.

Rowlingson, R. (2004). A Ten Step Process for Forensic Readiness. *International Journal of Digital Evidence, 2*(3).

Shedden, P., Ruighaver, A.B., Ahmad, A., 2010. Risk Management Standards – The Perception of Ease of Use. Journal of Information Systems Security. 6(3).

Strauss, A., & Corbin, J. (1994). Grounded theory methodology. *Handbook of qualitative research*, 273-285.

Tan, J. (2001). Forensic readiness. Cambridge, MA:@ Stake, 1-23.

Tan, T., Ruighaver, A.B., Ahmad, A. (2010). Information Security Governance: When Compliance Becomes more Important than Security. *Proceedings of The IFIP TC-11 24th International Information Security Conference (pp.55-67)*. Brisbane, Australia.

Taylor, M., Haggerty, J., Gresty, D., & Hegarty, R. (2010). Digital evidence in cloud computing systems. Computer Law & Security Review, 26(3), 304-308.

Valjarevic, A., & Venter, H. (2013). *Implementation guidelines for a harmonised digital forensic investigation readiness process model.* Paper presented at the Information Security for South Africa, 2013.

Wolfswinkel, J. F., Furtmueller, E., & Wilderom, C. P. (2011). Using grounded theory as a method for rigorously reviewing literature. *European Journal of Information Systems, 22*(1), 45-55.

Yasinsac, A., & Manzano, Y. (2001). *Policies to Enhance Computer and Network Forensics.* Paper presented at the Workshop on Information Assurance and Security - United States Military Academy, West Point, NY, US.

10. APPENDICES

Appendix 1: Elyas et al.'s (2014) DFR Framework Definitions

Capability	Definition
Regulatory Compliance	The ability of an organization to demonstrate adherence to laws and regulations (utilizing digital evidence in the context of forensic readiness).
Internal Investigations	The ability of an organization to produce evidence to facilitate internal digital investigations.
Legal Evidence Management	The ability of an organization to produce evidence that can be used in legal proceedings.

Factor	Definition
Strategy	An actionable plan designed to achieve forensic readiness in an organization.
Non-Technical Stakeholders	The individuals and/or parties, internal or external to the organization, who are not involved in the conduct or support of the forensic program of an organization.
Technical Stakeholders	The individuals and/or parties, internal or external to the organization, who are involved in the forensic program of an organization.
Technology	The software and/or hardware that may be required in a forensic program.
Monitoring	Monitoring the system for anomalies to detect incidents in a timely manner.
System Architecture	The design of a system towards maximizing its forensic potential.
Policy	A written set of principles designed to guide and manipulate behaviour within an organization for forensic purposes
Training	The process of educating staff members on their roles and responsibilities towards the forensic program.
Culture	A set of shared values, beliefs, assumptions and practices that shape and direct members attitudes and behaviour towards forensic readiness.
Top Management Support	Support of forensic readiness by the senior management of an organization.
Governance	The implementation of processes and structures in the organization that enable forensics.

Relationship	Description
C1: Forensic Readiness Capabilities – Forensic Strategy	There is a bidirectional relationship between Forensic Strategy and Forensic Readiness Capabilities that can be achieved. In order to achieve the capabilities, the organization must develop a Forensic Strategy. On the other hand, the type of strategy an organization develops influences the capabilities that can be achieved.
O1: Top Management Support – Forensic Strategy	There is a bidirectional relationship between Top Management Support and the Forensic Strategy. The top management of the organization authorise the activities of the forensic program and allocate funds. Once the forensic strategy is developed, the members of the senior management are expected to comply with its directives.
O2: Governance – Forensic Strategy	There is a bidirectional relationship between Governance and the Forensic Strategy. Governance ensures the efficiency of the forensic program (i.e. well-qualified personnel are hired, appropriate technologies are utilised, etc). On the other hand, changes in the strategy may lead to changes on the way governance is implemented.
O3: Culture – Forensic Strategy	There is a bidirectional relationship between Culture and Forensic Strategy. It is important to create an organizational culture where members of the staff believe in and appreciate the forensic initiative, so that they are more likely to adhere to its directives. On the other hand, implementing the Forensic Strategy will lead to changes on the existing organisational culture.
S1 & S2: Policy – Technical & Non-technical Stakeholders	Policy is connected to both Technical and Non-technical Stakeholders by two bidirectional relationships. The Policy document is developed through cooperation between the Technical and Non-technical Stakeholders. Once the policy is approved, both Technical and Non-technical stakeholders are expected to comply with.
S3: Technical Stakeholders – Non-technical Stakeholders	There is a bidirectional relationship between Technical and Non-technical Stakeholders. Incidents are communicated by Non-technical Stakeholders to a predetermined point of contact administered by Technical Stakeholders. On the other hand, Technical Stakeholders communicate with Non-technical Stakeholders when gathering information about incidents.
S4 & S5: Training – Technical & Non-technical Stakeholders	Training is connected to both Technical and Non-technical Stakeholders by two bidirectional relationships. The training program is designed by Technical and Non-technical Stakeholders. Further, Training may be conducted by the Technical Stakeholders. However, all staff (Technical and Non-technical) are expected to undergo certain level of Forensic Training.

S6, S7, & S8: Technical Stakeholders – Technology, Monitoring, & Architecture	Technical Stakeholders are linked to Technology, Monitoring, and Architecture by three unidirectional relationships. Forensic technologies are utilised by the Technical Stakeholders to perform their forensic tasks. The organizational system is actively monitored by Technical Stakeholders (e.g. system administrators) in order to detect incidents in a timely manner. Finally, the forensically architected system provides digital evidence that can be utilised by the Technical Stakeholders when needed.

Appendix 2: Focus Group Questions

First Focus Group Protocol

Section 1. General Questions

1. What is digital forensic readiness?
2. What objectives can an organization achieve by being forensically ready?
3. How could an organization become forensically ready?
    a. Where do you start?
    b. What is a "good" forensic program?
    c. What can security learn from forensic readiness?
    d. How does learning happen in forensic readiness?

Section 2. Case Scenario

Participants were given a case scenario and were asked to discuss the scenario in terms of the following:

1. What needs to be considered in a forensics readiness plan?
2. Who might be involved in a forensics readiness program?
3. What kind of technologies might be required in a forensics program?
4. Would monitoring the play a role in a forensics readiness program?
5. What kind of activities would company A need to take into consideration in order to optimize their forensics readiness? Would forensics readiness influence system setups?
6. Would the organization need to have a forensics policy?
7. Would the organizational staff need to be trained on forensics?
8. What constitutes best practice in forensics within an organization?
9. What role can senior management play in a forensics program?
10. Does governance have a role in forensic readiness?

Section 3. Diagram Presentation

The forensic readiness diagram is presented to the participants. The participants were then asked the following questions based on the diagram:

1. Can you identify additional forensic readiness objectives?
2. Can you identify additional factors that would influence an organizations forensic strategy?
3. Do you agree with the relationships depicted between the components of forensic strategy shown?
4. Does Organizational Forensic strategy influence forensic readiness objectives?

Second Focus Group Protocol

Section One: Generic Questions

Similar to the first, the second focus groups begins with generic questions about forensic readiness objectives and factors, to capture the unbiased opinion of the participants regarding the phenomenon. The following questions were asked:

- What is organizational digital forensic readiness?
- What does an organization gain by being forensically ready? In other words, what are the benefits of being forensically ready organization?

Section Two: Expert Opinion on the Proposed Objectives and Factors

Form-based questions are handed over to the participants for parts 2-5 of the focus group. The three forensic readiness objectives and ten factors are presented to the participants. The participants are asked whether they agree or disagree with these categories, and to provide justifications.

Forensic Readiness Objectives

- We believe there are three main objectives that are improved by adopting forensic readiness.
- Please indicate whether you agree or disagree with these objectives on the handout, and provide your reasoning.
- If you think that there are other objectives please add them to the handout.

Forensic Readiness Factors

- We have found ten key factors contributing to forensic readiness.

- Please indicate whether you agree or disagree with these factors on the handout, giving your reasons.

Section Three: Completeness of the Factors

A List of DFR Factors and Objectives is presented. The participants are asked to add factors / objectives they believe are missing. These are then discussed between all the participants.

Section Four: Model Relationships (Expert's Perspective)

Two identical lists of the ten factors are presented to the participants. They are asked to add any factors they proposed in the last section, to the blank spaces of the list. The participants are then asked to draw the top 8 relationships between the factors in the two lists. The purpose is to find out the most significant relationships within the model from expert's point of view.

Section Five: Model relationships (the proposed model)

Finally, the proposed forensic readiness model (with relationships) is presented. The proposed relationships are described in the given questionnaire form. The participants are asked whether they agree or disagree with the proposed relationships and their descriptions. The participants are also asked if they think any key relationships are missing.

Third Focus Group Protocol

The protocol of the third focus group consists of four sections.

Section 1: Generic Questions

The focus group begins with generic questions about forensic readiness.

- What is organizational digital forensic readiness?
- What does an organization gain by being forensically ready?
- How does an organization become forensically ready?

Section 2: Forensic Readiness objectives

Form-based questions are distributed to the participants. The proposed forensic readiness objectives are described in the form. The participants are asked to indicate whether they agree or disagree with the objectives as described and provide justifications. The participants are also given a space to add more objectives, if they believe any are missing. Participants now discuss the objectives with one another.

Section 3: Forensic Readiness Factors

Form-based questions are distributed to the participants. The proposed forensic readiness factors are described in the form. The participants are asked to indicate whether they agree or disagree with the factors as described and provide justifications. The participants are also given a space to add more factors, if they believe any are missing. Participants now discuss the factors with one another.

Section 4: The forensic Readiness Model (Relationship)

The proposed forensic readiness model is presented to the participants. The proposed relationships are described in the given form. The participants are asked whether they agree or disagree with the proposed relationships and their descriptions, and to provide justifications for their response. They then discuss their answers with one another.

Section 5: Concluding Questions

The session concludes with the following questions:

- Are there any additional relationships that you think should be represented in the framework?
- Do you think that the framework accurately represents the capability of forensics within an organization?
- How do you think the framework could be used by organizations?

Appendix 3: Refined DFR Framework Definitions and Descriptions.

Forensic Readiness Objective	Short Definition	Description
Regulatory Compliance	Being able to demonstrate adherence to laws and regulations	In many legal and regulatory jurisdictions, organizations are required to be capable of responding to incidents, ensuring that incidents are reported, making their data discoverable, retaining financial records, etc. Being forensically ready helps organizations satisfy these requirements. It also helps in providing evidence of compliance with non-forensic related regulations.
Forensic Response	Being able to initiate forensic investigations, and forensically responding to incidents at reduced costs	Forensic response to incidents may range from simply knowing what had happened, to running full internal investigations. A forensic capability would enable organizations to run their own digital investigations and producing relevant and reliable digital evidence in a timely manner with less costs.
Legal Evidence Management	Being able to produce legally sound digital evidence	Organizations may be required to produce digital evidence for legal proceedings, such as: prosecution, legal defense, e-discovery orders, and commercial disputes. Being forensically ready improves the chances of organizations to provide such evidence
Business Objectives	Refers to objectives that are not directly related to forensics, but are achieved by adopting forensic readiness	Business objectives may include: improving the security strategy based on the outcomes of investigations, maintaining the reputation of the organization, reducing investigation costs, reducing disruption of investigations on business, improving the interaction interface with law enforcement, evaluating the impact of incidents, and being able to recover data.

Forensic Readiness Capability	Short Definition	Description
Forensic Strategy	An actionable plan designed to achieve forensic readiness in an organization	Organizations will use the forensic strategy to achieve their forensic readiness objectives. Typically the forensic strategy will include: forensic policy, forensic training, forensic infrastructure, and will employ forensic and non-forensic stakeholders. The forensic strategy must be flexible to adapt to changes in the organizational environment, and will be unique to individual organizations.
Forensic Stakeholders	Internal or external parties directly involved in forensic activities	Forensic stakeholders may include system and network administrators, external consultants and others that are co-opted in a forensic role as required (e.g. policy writers, trainers, legal personnel). Forensic stakeholders play a central and critical role in the framework as they represent the human resources required in the forensic program.
Non-forensic Stakeholders	Internal or external parties indirectly involved in forensic activities	Non-forensic stakeholders include all internal and external parties not directly involved in forensic activities. It is important that non-forensic stakeholders become aware of, and adhere to the forensic policy and best practice. For example, in the event of an incident, the policy may require employees not to turn off a compromised computer. Lack of awareness at the non-forensic stakeholders end, may hinder the organizational forensic efforts.
Forensic Technology	Software and hardware used in the forensic program to capture, preserve, analyse, and/or report forensic evidence	Forensic technologies may include analysis tools such as EnCase, and capture software such as logging and event reporting tools. Forensic technologies are essential to perform the forensic tasks.
Forensic Architecture	The design and configuration of technology infrastructure for forensic purposes	Design involves the placement of various forensic technologies within the overall network and systems environment. Configuration is methodological process by which forensic technologies are customized to enable forensics within the overall network and systems environment. The organization's technology infrastructure must be architected in a way that increases its production, retention, and protection of potential digital evidence.
Forensic Policy	A set of procedures and guidelines designed to encourage forensically sound behaviour within an organization	The policy document outlines forensically sound behaviour for forensic and non-forensic stakeholders. For example the policy will include procedures on how to conduct a forensic investigation which will be relevant to forensic stakeholders. The policy will also include how non-forensic stakeholders should handle computing equipment when they suspect a forensic incident.
Forensic Training	Teaching organizational staff how to comply with forensic best practices	Different sets of training may be offered to the different staff of an organization based on their roles in the forensic program. For instance, technical forensic stakeholders will require professional forensic training, while non-forensic stakeholders may only need awareness training as well as basic training on how to handle computing equipment and evidence.

Forensic Readiness Capability	Short Definition	Description
Forensic Culture	A set of shared values, beliefs, assumptions, and practices that shape and direct members' attitudes and behaviours towards forensic readiness	If the organizational culture is not supportive of forensics, this may jeopardise the entire forensic initiative. The implementation of a forensic readiness program shall be accompanied by a cultural change in the organization towards forensic best practice. This change may be cultivated through training and policy implementation.
Top Management Support	Support of the forensic program by the senior management of an organization	Support of the senior management of the forensic program is indispensable. Senior management must support the forensic program as an organization-wide initiative. Support may include: funding, decision making, process authorization, policy enforcement, staffing, resource allocation, and oversight.
Forensic Governance	The implementation of processes and structures in the organization that set the responsibilities and practices within the forensic program	Governance in the context of forensics refers to the admipangreddration and management of a set of procedures and responsibilities pertaining to any evidence found in computers and other organizational digital resources that may have legal value, as facilitated by executive management. Governance is important to ensure the quality of the forensic program.

Appendix 4: Description of Relationships

Relationships	Description
R1: Forensic Readiness Capability – Forensic Readiness Objectives	The relationship between Forensic Readiness Capability and Forensic Readiness Objectives is bi-directional. In order to achieve forensic readiness objectives, an organization needs to develop a forensic readiness capability. Similarly, an organization's forensic readiness capability will vary depending on the particular readiness objectives targeted. For instance, if the objective of an organization is to ensure that legal evidence is managed correctly, so that it stands up in a court of law rather than be used for internal purposes, then legal rules of evidence and standards of reliability must be considered in strategy development. Therefore, we suggest that forensic readiness capabilities and forensic readiness objectives influence each other.
R2: Forensic Strategy – Organizational Factors	Organizational factors refer to top management support, governance, and culture. The relationship between forensic strategy and organizational factors is bidirectional and represents the support that organizational factors provide for forensic strategy as well as how the forensic strategy may influence the organization. For example, having support from top management, a good governance structure, and facilitative culture will have a positive effect on the forensic strategy. Conversely, the forensic strategy influences the perception of top management and affects the culture and governance of the organization.
R3: Forensic Stakeholders – Forensic Policy	The relationship between forensic stakeholders and forensic policy is bi-directional, as it represents that whilst the forensic stakeholders develop the forensic policy, they must also abide by it.
R4: Forensic Stakeholders – Forensic Training	The relationship between forensic stakeholders and forensic training is bi-directional, as forensic stakeholders develop forensic training and also undertake training. For example, forensic stakeholders will develop general forensic training for the non-forensic stakeholders, whilst undertaking outsourced specialized forensic training.
R5: Non-forensic Stakeholders – Forensic Policy	The relationship between non-forensic stakeholders and forensic policy is bi-directional. The forensic policy dictates appropriate forensic behaviour of non-forensic stakeholders. On the other hand, policy development is influenced by the non-forensic stakeholders. For example they may provide feedback on the effectiveness of the policy, which may be used to improve policies as part of the development process.
R6: Non-forensic Stakeholders – Forensic Training	The relationship between non-forensic stakeholders and forensic training is bi-directional. The non-forensic stakeholders in the organization need to undergo regular forensic training. Conversely, the feedback and performance of the trainees may influence how training is designed and delivered in the future.
R7: Forensic Stakeholders – Non-forensic Stakeholders	The relationship between forensic stakeholders and non-forensic stakeholders is bi-directional. For example, non-forensic stakeholders may initiate communication with the forensic stakeholders in the event of a forensic incident. Similarly, forensic stakeholders may initiate communication with the non-forensic stakeholders in the conduct of a forensic investigation, forensic training, etc.
R8: Forensic Stakeholders – Forensic Infrastructure	There is a unidirectional relationship from forensic stakeholders to forensic infrastructure. Together, forensic technology and forensic architecture form the forensic infrastructure of an organization. The forensic stakeholders design the forensic architecture which incorporates the selection of forensic technologies. The architecture and technology are then utilized by the technical forensic stakeholders to achieve the forensic tasks.