2017

# Are You Ready? A Proposed Framework For The Assessment Of Digital Forensic Readiness

Andres Felipe Diaz Lopez
*University of Mississippi*

Recommended Citation
Diaz Lopez, Andres Felipe, "Are You Ready? A Proposed Framework For The Assessment Of Digital Forensic Readiness" (2017). *Electronic Theses and Dissertations*. 1061.
https://egrove.olemiss.edu/etd/1061

# ARE YOU READY?

# A PROPOSED FRAMEWORK FOR THE ASSESSMENT OF DIGITAL FORENSIC READINESS

A Dissertation

Presented in Partial Fulfillment of Requirements

For the degree of

Doctor of Philosophy in Business Administration

Management Information Systems

The University of Mississippi

Andrés Felipe Díaz López

August 2017

# ABSTRACT

This dissertation develops a framework to assess digital forensic readiness (DFR) in organizations. DFR is the state of preparedness to obtain, understand, and present digital evidence when needed. This research collects indicators of digital forensic readiness from a systematic literature review. More than one thousand indicators were found and semantically analyzed to identify the dimensions to where they belong. These dimensions were subjected to a Q-sort test and validated using association rules, producing a preliminary framework of DFR for practitioners. By classifying these indicators into dimensions, it was possible to distill them into 71 variables further classified into either extant or perceptual variables. Factor analysis was used to identify latent factors within the two groups of variables. A statistically-based framework to assess DFR is presented, wherein the extant indicators are used as a proxy of the real DFR status and the perceptual factors as the perception of this status.

## DEDICATION

A mi mamá

## LIST OF ABREVIATIONS AND SYMBOLS

| | |
|---|---|
| ACON | Extant Active Control |
| BACK | Extant Backup Resourcing |
| BURD | Perceived Burden |
| CDE | Comprehensive Digital Evidence |
| CERT | Computer Emergency Response Team |
| COMM | Perceived Organizational Commitment |
| CULT | Perceived DFR Culture |
| DCOC | Digital Chain of Custody |
| DE | Digital Evidence |
| DF | Digital Forensics |
| DFI | Digital Forensic Investigation |
| DFMF | Digital Forensic Management Framework |
| DFR | Digital Forensic Readiness |
| DFRMS | Digital Forensic Readiness Management System |
| DFRWS | Digital Forensics Research Workshop |
| EEDI | End-to-End Digital Investigation |
| EMBD | Extant DFR Embeddedness |
| EMP | Evidence Management Plan |
| EXPO | Perceived Exposure |
| EXT | Extant (Factor/Indicator) |
| FRP | Forensic Readiness Policy |
| IA | Information Assurance |

| | |
|---|---|
| IAAC | UK Information Assurance Advisory Council |
| IDS | Intrusion Detection System |
| IEXP | Extant Incident & Evidence Expertise |
| INFO | SEC Information Security |
| INVE | Extant Investigative Capacity |
| IS | Information Security |
| NFR | Network Forensic Readiness |
| NTP | Network Time Protocol |
| PDFR | Perceived Perceived DFR |
| PER | Perceptual (Factor/Indicator) |
| POLI | Extant Policing |
| ProDF | Proactive Digital Forensics |
| RESP | Perceived Perceived Response Control |
| SEM | Security Event Management (software) |
| SPF | Security Policy Framework |
| SPOC | Single Point of Contact |
| TECH | Extant Technological Capacity |
| WIRE | Extant Wireless Accessibility |

## ACKNOWLEDGMENTS

I want to thank the members of my dissertation committee, Doctors Brian Reithel, Milam Aiken, Bart Garner and Walter Davis for being part of this project, for their teachings and for their permanent support. Dr. Reithel, as my advisor, has been fundamental for the successful completion of this work and continues to be my reference in my professional career.

The encouragement of my family and friends has been very important during this process. To those, who keep their unwavering confidence in me and feel like yours my failures and successes, my infinite gratefulness. This achievement is also yours.

“La motivación de mi familia y amigos ha sido muy importante durante este proceso. Para aquellos que han mantenido su inquebrantable confianza en mí y sienten suyos mis éxitos y fracasos, mi infinita gratitud. Este logro es suyo también.”

## CONTENTS

## LIST OF TABLES

## LIST OF FIGURES

# CHAPTER I

# INTRODUCTION

The use of information systems generates traces of all kinds due to activities exerted by humans as well as by computers. The art of discovering, collecting, managing and reporting this digital evidence is called digital forensics and has become a discipline of increasing importance for governments and organizations alike. John Tan (2001) described the different measures that can be taken in order to prepare systems to reduce the digital forensic work required to recover from an incident, and collect information to detect the source of the attack and reduce the system's vulnerabilities. Tan's paper is called "forensic readiness" and he is commonly credited with the coining and definition of this term. The present dissertation builds over Tan's and many other authors' works on digital forensic readiness to offer a quantitative assessment of the ability of organizations to provide digital evidence when needed.
Tan's seminal paper recounts that during the Honeynet Project, 13 subjects participated in a contest in which they reported findings of their forensic analysis on disk images of a compromised honeynet system. The head of the project, Dave Dittrich noticed that on average, two hours of intruder time turned out to mean 40 billable hours of forensic identification. This did not include: intrusion detection (human element), forensic acquisition of disk images, restoration of the compromised system, hardening of the compromised system, network scanning for other vulnerable systems, and communications with stakeholders (Tan 2001).

Forensic readiness measures have emerged as a response to the situation described by Tan, and as a complement to the traditionally reactive approach used in digital forensics. "Digital Forensics is a discipline that primarily focuses on the post-incident side of an investigation. However, during the last decade, there is a considerable amount of research that considers proactive measures taken by organizations. Such measures comprise a digital forensic readiness plan" (Mouhtaropoulos, Grobler, & Li 2011). Today forensic readiness is an indispensable part of the digital forensics discipline.

The development of digital forensics has not been free of challenges. On one hand, there has been a slow and complex process in adapting the legal framework to the admissibility of evidence stored and processed by computers and networks. On the other hand, companies are reluctant to disclose information that may cast doubts on their ability to control the security of their assets. A small percentage of hacker attacks are reported; 26% on non-reporters fear bad publicity, 22% believed law enforcement couldn't help, and 14% think competitors would use it in their favor (Pangalos, Ilioudis & Pagkalos 2010). Still, being able to assess and improve the forensic readiness status of organizations is a highly desired goal with clear benefits. Better preparedness reduces the occurrence of incidents and the associated excessive costs of corrective actions. Moreover, measures taken within an adequate program for forensic readiness enhance the weight of the digital evidence before courts of law. Additionally, organizations seeking forensic readiness are in better control of the situation when digital incidents occur. They would be able to manage many situations without the help of official security forces; hence, reducing the need to disclose their vulnerabilities before law enforcement and the public.

Despite these benefits, organizations do not have standard mechanisms to assess this readiness. "Digital forensic readiness is often ad hoc and no consistent application or framework exists globally. As a result, there is no standard way to specify computer system's forensic capabilities or to formally compare systems" (Mouhtaropoulos, Grobler, & Li 2011), and rather, a lack of maturity in the discourse that is rooted in the reliance on informal definitions of key terms and concepts (Elyas, Ahmad, Maynard & Lonie 2015). In consequence, Pangalos & Katos (2010) ask for security policies to be assessed for their forensic readiness status, and suggest the need of a metric of forensic readiness to achieve this.

The present paper seeks to produce such a framework and develop a mechanism to assess the digital forensic readiness in organizations. This endeavor is undertaken through a process divided in two phases. In phase one, the extant literature in digital forensic readiness (DFR) is systematically reviewed to understand the concept of DFR and extract its potential indicators and dimensions. A preliminary framework, tested through Q-Sorting among independent qualified reviewers and validated using association rules, is revealed. This can be considered a practitioners' framework of DFR, not yet the theoretical framework seeked for by this research. Phase two uses the discovered dimensions to further synthesize the indicators into measurable variables. These variables are tested in a pilot study among a small sample of organizations. The pilot study assesses the feasibility of the survey in terms of length, clarity of the questions, and adequacy of the results to be analyzed via exploratory factor analysis. Once the survey is refined and adjusted, a bigger sample of organizations is surveyed and factor analysis is run again in order to discover the latent factors that explain DFR.

The systematic review of the extant literature on DFR is deemed the most comprehensive mechanism to extract potential indicators of a specific status of DFR in organizations. This process includes the discovery of: 1) the different terms associated to digital forensic readiness, 2) the purposes for which this readiness is sought, 3) the steps and requirements for achieving certain status of forensic readiness and 4) the previous attempts to define a framework of factors that determine the digital forensic readiness capability of organizations. This information is aggregated, refined and sorted using structured techniques such as the Q-Sort test.

The application of quantitative techniques as a means to elaborate the digital forensic readiness framework distinguishes this work from previous proposals, which have implemented qualitative approaches to build the framework. Furthermore, the present research proposes a framework that can be used both as an instrument for the implementation of DFR measures and as an instrument to measure DFR levels at specific moments. To the best of the researcher's knowledge, this is the first time this subject is addressed with a quantitative approach.

The general hypothesis of this research is that the framework to assess DFR can be developed using quantitative techniques such that a number of identifiable factors might suggest the level of DFR of an organization; it is, to be able to present valid digital evidence whenever it is required to do so. Furthermore, other factors, representing the perception about this readiness, and their correlation with the former, can also be discovered. The definition of these factors and their relationships constitute the DFR framework looked for by this research.

# CHAPTER II

# LITERATURE REVIEW

Digital Forensic Readiness is a term in the making. Different terms in the literature have been used to describe similar concepts and different descriptions are found to refer to equivalent terms. In addition, the domain of the concept has extended to different disciplines, objectives and stakeholders, making it, heretofore, an unstandardized, yet vital, measure for organizations. The following sections are used to explain this and other associated terms as they show up in the literature. Given that digital forensic readiness is considered part of the wider discipline of digital forensics, this term is explained first.

## Digital Forensics

"Digital Forensics can be defined as the efficient use of analytical and investigative techniques for the preservation**,** identification, extraction, documentation, analysis, and interpretation of computer media which is digitally stored or encoded for evidentiary and/or root-cause analysis and presentation of digital evidence derived from digital sources for the purpose of facilitation or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations" (Grobler & Louwrens 2007). "Digital evidence is present in disputes and crimes where (i) computers and the information they store have been targeted, (ii) computers have been used as tools, and (iii) computers have been used as repositories for information used or generated in the commission of crimes or disputed events" (Danielsson & Tjøstheim 2004).

The concept of digital forensics has experienced evolution in regards to the appropriate term and the corresponding definition. Law, on one hand, and informatics, on the other, are the two disciplines that converge in the initial development of this discipline. Digital forensics is closely associated to the management and legal treatment of "electronically stored information (ESI)," which is also known as digital evidence (e.g. Richard 1999).

On the legal side, the U.S. “Federal Rules of Civil Procedure (FRCP) were amended in 1970 to acknowledge the widespread use of computers by allowing for discovery of electronic media in addition to traditional forms of printed media” (Youst & Koh 1997). On the technology side, works such as “Secure Audit Logs to Support Computer Forensics” (Schneier & Kelsey 1991), “Forensic Readiness” Tan (2001), “Investigating Sophisticated - Security Breaches” (Casey 2006), among others have been developed in order to guide the collection and production of electronic evidence. Garfinkel (2010) says that 1999 to 2007 is kind of the “Golden Age” for digital forensics due to the realization of our ability to see the past through the recovery of residual data.

One of the first terms used instead of digital forensics was “forensic computing” (e.g. McKemmish 1999; Wolfe-Wilson & Wolfe 2003) referred to as “the methodologies used to capture and authenticate data at its source, analyse that captured data for evidence relevant to the case at hand, produce an understandable report that can be introduced into evidence in a court of law, and testify as to the authenticity of evidence presented” (Wolfe-Wilson & Wolfe 2003). Kent, Chevalier, Grance & Dang (2006) notice that digital forensics is also known as computer and network forensics, and has many definitions. “Generally, it is considered the application of science to the identification, collection, examination, and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data. It comprises four basic phases: collection, examination, analysis, and report” (Kent, Chevalier, Grance & Dang 2006).

This definition includes the application of science in response to courts’ requirements for the admissibility of evidence, which is a major challenge for presenting digital data before courts of law. For example, the Daubert test asks for the recognitions, testability, error rate, and acceptance of the technique producing the evidence for its admissibility. “We might extend the common definition of forensic science, in the case of digital forensic science, as the application of computer science and mathematics to matters of law” (Stephenson 2003).

Some practitioners might consider the limitation of digital forensics to evidence that has the potential to be used in courts of law as inconvenient compared to the practical use of digital forensics. Broader definitions may be preferred. For example, when used to detect nosey people accessing data they are not supposed to access. “Determining what is an act of curiosity and what is a genuine access of confidential records is a subjective issue" (Hoolachan & Glisson 2010). Hoolachan & Rowlingson (2001) contend that forensic readiness "is that an organisation can pre-empt the occurrence of a crime by preparing the environment in advance and in doing this, organisations will benefit not only in instances where prosecution becomes an issue, but also in limiting their own business risks" (Pooe & Labuschagne 2012).

Two more definitions support this broader view of digital forensics. The first one says that "digital forensics comprises analytical and investigative techniques used for the preservation, identification, extraction, documentation, analysis and interpretation of computer media, which are digitally stored or encoded for evidentiary and/or root cause analysis" (VonSolms, Louwrens, Reekie & Grobler 2006). In the second, Whitcombe (2002) says that digital forensics refers to digital evidence, understood to be any information of probative value that is either stored or transmitted in a digital form (Bem, Feld, Huebner & Bem 2008).

Some authors also coincide in that digital forensics can also include evidence not stored in computers: "many of the issues facing digital security exist in a non-digital medium (Hoolachan & Glisson 2010). Bem et al. (2008) explain that digital forensics "refers not only to computers, but also to digital audio and video, digital fax machines, and similar." They also propose seven components of incident response of which the Pre-incident preparation stage has been matched to forensic readiness.

No agreement in the models used to approach digital forensic investigations, perhaps due to the lack of technology neutrality of some proponents of such frameworks (Beebe & Clark 2005). In the next section different approaches for the decomposition of the digital forensic investigation process are presented as a starting point in defining the concept of digital forensic readiness.

### Digital Forensics Investigation Process

At a very high level every digital forensic investigation must go through the following phases:

1. Define the scope and goals of the investigation
2. Determine the work and materials
3. Acquire the images of the devices to be examined
4. Perform the digital forensic analysis
5. Prepare the report (Ngobeni, Venter & Burke 2010)

An evidence-centered view of the digital forensic investigation (DFI) process includes 5 phases:

1. Identification
2. Collection
3. Transportation
4. Storage
5. Examination and presentation (Trenwith & Venter 2013)

For the Digital Forensics Research Workshop (DFRW) - a large-scale consortiums lead by academia rather than law enforcement - that process includes 7 stages:

1. Identification
2. Preservation
3. Collection
4. Examination
5. Analysis
6. Presentation
7. Decision (Reith, Carr & Gunch 2002)

Chen, Tsai, Chen & Yee (2005), combine the high level and evidence-centered approaches in a cycle of 7 stages:

1. Officially accept a fact or an object to be examined
2. Plan a forensics procedure for producing a legally admissible report
3. Carry out the forensics process
    3.1 Evidence
    3.2 Identification
    3.3 Analysis
    3.4 Verification
    3.5 Individualization
    3.6 Crime scene reconstruction
4. Collect forensics results
5. Analyze the forensics results

6. Present the forensics results and compile a forensics report

7. Determine the evidential effect

Bem et al. (2008) also say that there are “seven components of incident response, but they moved the planning to the initial stage:

1. Pre-incident preparation

2. Detection of incident

3. Initial response

4. Formulate response strategy

5. Investigate the incident: data collection followed by analysis

6. Reporting

7. Resolution (lessons learned, long-term solutions)

Other stages of the digital forensic investigation process different to those described by Bem et al. (2008) are proposed by different authors. For example, Kruse & Heiser (2002) summarize the phases of the digital forensic process in:

1. Securing the evidence without contaminating it

2. Acquiring the evidence without altering or damaging the original

3. Authenticating that the recovered evidence is the same as the original seized data

4. Analyzing the data without modifying it

However, VonSolms, Louwrence, Reekie & Grobler (2006) point out the reactive nature of this approach lacking planning and preparation. Thus, they propose a sequence of:

1. Planning and preparation

2. Incident response

3. Investigation and juridical/evidentiary

What we can infer form these different approaches is that literature supports that DFR is a first stage in the DFI process. DFR is defined as the preincident plan within the DF lifecycle that deals with digital evidence identification, preservation, and storage whilst minimizing the costs of a forensic investigation” (Mouhtaropoulos & Li 2012).

Carrier & Spafford (2003) make a parallel between the physical and the digital investigations and mention different approaches of these processes in order to offer a summarized view. For example, Prosise & Mandia (2001) propose an investigation sequence comprised by:

1. Detection of the Incident
2. Initial Response
3. Response Strategy Formulation
4. Duplication
5. Investigation
6. Secure Measure Implementation
7. Network Monitoring
8. Recovery
9. Reporting
10. Follow-up (Carrier & Spafford 2003)

Whereas the Department of Justice (DoJ) proposes a process following:

1. Preparation
2. Collection
3. Examination
4. Analysis
5. Reporting (Carrier & Spafford 2003)

And the US Air Force considers a sequence of stages involving:

1. Identification
2. Preparation
3. Approach Strategy
4. Preservation
5. Collection
6. Examination
7. Analysis
8. Presentation

9. Return Evidence (Carrier & Spafford 2003)

After considering these approaches, Carrier & Spafford proposed a comprehensive set of 17 phases into 5 groups:

1. Readiness Phases
   - Operations Readiness
   - Infrastructure Readiness
2. Deployment Phases
   - Detection and Notification
   - Confirmation and Authorization
3. Physical Crime Scene Investigation Phases
   - Preservation
   - Survey
   - Documentation
   - Search and Collection
   - Reconstruction
   - Presentation
4. Digital Crime Scene Investigation Phases
   - Preservation
   - Survey
   - Documentation
   - Search and Collection
   - Reconstruction
   - Presentation
5. Review Phase
   - Review

This model of the digital investigation process has been adopted by later authors (e.g. Rowlingson 2004; Mouhtaropoulos & Dimotikalis 2013; Mouhtaropoulos & Li 2012) with zero or few modifications. In fact, Mouhtaropoulos & Dimotikalis (2013) and Mouhtaropoulos & Li (2012) use the model to define DFR as “the preincident plan within the digital forensics lifecycle that deals with digital evidence identification, preservation, and storage whilst minimizing the costs of a forensic investigation” (Mouhtaropoulos & Dimotikalis 2013). A subtle variation of Carrier & Spafford’s model can be seen in forensiccontrol.com, where the digital forensic process is divided into 6 stages:

1. Readiness
2. Evaluation
3. Collection
4. Analysis
5. Presentation
6. Review

Pollitt (2007) does a review of some of these and other process models of digital forensics and reminds us that there are different knowledge management contexts involved in them. They are the physical, the logical and the legal contexts. Likewise, Pollitt shows that Mocas (2003) also identifies other contexts for the analysis of digital forensics. They are law enforcement context, a military context and a business system security context.

Regardless of the conceptual model of digital forensics used, we can see digital forensic readiness as an initial state of this general digital forensic process that is becoming more relevant due to its implications in later stages and the costs associated to a complete investigation. “Proactive digital forensics is a phase within the digital forensics lifecycle that deals with pre-incident preparation. (Mouhtaropoulos, Li & Grobler 2012). In the next section, the concept of digital forensic readiness is explored.

### Conceptual Approaches to Forensic Readiness

The oldest antecedent of the term forensic readiness is found in John Tan’s paper “Forensic Readiness” of 2001. He defines the concept by stating its 2 objectives:

1. Maximizing the environment’s ability to collect credible digital evidence, and
2. Minimizing the cost of forensic during an incident response.

In this seminal paper the elements of forensic readiness are listed as:

1. How Logging is done

2. What is logged

3. Intrusion Detection Systems (IDS)

4. Forensic acquisition

5. Evidence handling

The paper also describes 4 potential sources of incident data, which are:

1. The victim's RAM

2. The attacker's RAM

3. The intermediary system's logs

4. The physical security (For example, cameras)

In consequence, Tan gives recommendations to incident management in Windows and Unix operating systems and explains that the digital data from an intrusion can be used with diverse purposes, such as a leverage in an internal incident or evidence in court, as a base for formulating response plans during an incident response or to look for additional vulnerability and compromise, and even as an auto incriminating evidence (Tan 2001).

Robert Rowlingson (2004) developed a commonly cited definition of forensic readiness (i.e., Grobler & Louwrens 2007; Reddy & Venter 2009) that says that it "is the ability of an organisation to maximise its potential to use digital evidence whilst minimising the costs of an investigation;" and adds "forensic readiness is a security process which is more procedural and staff-intensive than technological".

Garcia (2005) modified Rowlingson's definition to describe forensic readiness as the "art of maximizing the environment's ability to collect credible evidence" (Pooe & Labuschagne 2012). Spike Quinn (2005) is even more concise and defines forensic readiness as being prepared to deal effectively with events that may require forensic investigation. While appropriate, Quinn's definition allows interpretations outside the context of digital systems. In contrast, Rowlingson's definition fits the context of computerized systems.

Other terms such as "proactive computer system forensics" and "network forensic readiness" are also used in agreement with the context of DFR as defined by Tan (2001) and Rowlingson (2003). In the present paper the term Digital Forensic Readiness (DFR) is considered a more appropriate term to denote the concept expressed by Tan and Rowlingson. However, the similarities among these terms are evident and it can be expected that authors refer to digital forensic readiness with other names.

For instance, instead of forensic readiness, some authors use the concept of proactive forensics: “proactive computer system forensics is the design, construction and configuring of systems to make them most amenable to digital forensics analyses in the future” (Bradford, Brown, Perdue & Self 2004). Mouhtaropoulos & Dimotikalis (2013) highlight the equivalence of the concepts “proactive forensic capability” and “digital forensic readiness” by saying that “little academic research has been conducted on an organization's proactive forensic capability. This capability is referred to as digital forensic readiness and aims to maximize the forensic credibility of digital evidence, while minimizing its post-incident forensic investigation.”

Another term, network forensic readiness (NFR), is defined as "maximizing the ability of an environment to collect credible digital evidence while minimizing the cost of an incident response” (Endicott-Popovsky, Frincke & Taylor 2007). Although constrained to the specific context of networks, this definition is very similar to the general concept of forensic readiness given the hyper connectivity of current systems. Yet, later papers (e.g. Taylor, Endicott-Popovsky & Frincke 2007; Forte 2010; Pangalos, Ilioudis & Pagkalos 2010) use the term forensic readiness.

One way to synthesize what is common to this diversity of terms used to denote the same concept is to define its scope. For example, the word “digital” seems to have a more comprehensive scope than the words “computer” and “network”.The following section addresses these issues of the scope of forensic readiness.

### Forensic Readiness’ Scope

The posterior development of the concept of forensic readiness has turned it into an organizational matter more than a matter of the technology used. Unlike information technologies, which include data, hardware and software, information systems include also people and procedures, and the management of this information systems must be aligned to the corporate strategy (Kroenke 2013). Forensic readiness is, then, understood as a state or capability of the organization’s information systems with special recognition of the role played by people and procedures, as shown in more recent definitions (e.g. Rowlingson 2004).

Forte describes the complexity of the forensic readiness implementation by adding that “planning and preparation involve the drafting of guidelines, procedures and standards, the development and preparation of training programs tailored to the various figures involved, and the selection and validation of technologies to use in incident response and digital investigation processes. It is also quite clear that these responsibilities entail keeping abreast of the state of the art in terms of both tools and skills, and keeping all documents hardware and software up to date” (Forte 2010).

Also, different authors stress the importance of legal (e.g. Grobler, Louwrens & Von Solms 2010a and b; Mouhtaropoulos, Grobler, & Li 2011) and financial (e.g. Tan 2001; Reddy, Venter & Olivier 2012) aspects in forensic readiness. (Taylor, Endicott-Popovsky & Frincke 2007) describe forensic readiness as “the capability of the system to efficiently collect credible digital evidence that can then be used in legal proceedings”. They explain that “efficiency for digital forensics has been described in terms of cost since costs tend to be significant, especially for systems that are not forensics ready”, and that “credible digital evidence refers to data that have been collected and preserved through a process that does not invalidate the legitimacy of the data”.

The use of the term digital forensic readiness (DFR) is more recent than the use of the term forensic readiness. However, the connotation remains the same, as shown by the research of Mouhtaropoulos, Grobler, & Li (2011), who explore different understandings of DFR in governments and the academia. Some of the illustrative assertions in their work are: “digital forensic readiness involves the identification, preservation and storage of digital evidence (DE)”, “Forensic readiness is cited as proactive digital forensics, a term introduced by Bradford, Brown, Purdue and Self to include all preventative security measures taken by a system”, and “Forensic readiness for a computer system, as defined by the US, is the capability of the system to efficiently collect credible digital evidence that can be used in legal proceedings”.

Two peculiarities of these statements must be noted. On one hand, there is a reference to “credible digital evidence”. On the other hand, it includes specific jurisdictions as a relevant characteristic of DFR. This is important because the word “forensics” implies “the use of science and technology to investigate and establish facts in criminal and civil courts of law”, which means that “the goal of any forensic investigation will be to prosecute the criminal or offender successfully, determine the root cause of an event and determine who was responsible" (Grobler & Louwrens 2007).

In consequence, the domain of DFR has been limited to only evidence that can be accepted in courts of law of specific jurisdictions. Because DFR is a stage of the digital forensic investigation (DFI) process, it is limited by the same legal boundaries for digital forensics made clear by authors such as Taylor, Endicott-Popovsky & Frincke (2007) and Trenwith & Hein S Venter [2013], who state "only evidence deemed to be legal and useful in building a case should be collected for analysis. This is referred to as the proportionality rule".

Although this view fits the semantics of the term, it is hardly appropriate to represent the cases that researchers have elaborated to denote forensic readiness. For example, Elyas, Ahmad, Maynard & Lonie (2015) found that "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". Clearly, not all tasks considered within the forensic readiness scope are meant to satisfy legal requirements. Non-legal uses of forensic readiness tasks are also ackowledged when they are referred to as "the implementation of preparatory measures that can immediately be put into effect in the event of an incident having implications regarding either for internal processes or legal compliance" (Forte 2010). Not all evidence to solve an internal disagreement would be strong enough for a court of law and not all evidence that is useful to detect additional vulnerabilities in the organization, as suggested by Tan (2001), would be of use in a trial.

Still, in an adaptation of Rowlingson's definition, digital forensic readiness is said to be "the ability of an organization to maximize its potential to use comprehensive digital evidence (CDE) whilst minimizing the costs of an investigation" (Grobler, Louwrens & Von Solms 2010), where authors propose the new term "Comprehensive Digital Evidence (CDE)" as "digital evidence that is complete, relevant, admissible, and have an evidentiary weight in a court of law to determine the root-cause of an incident and link the attacker to the perpetrator" (Grobler et al. 2010).

The extent to which either the definition or the term are to be adapted in order to facilitate the development of a standard measure of digital forensic readiness must be a primary endeavor for researchers. On one hand, limiting DFR to only evidence usable in courts dismisses the potential benefits of DFR measures in non-legal organizational affairs. On the other hand, including non-legal evidence increases the complexity of the concept and our ability to assess it.

This research considers that the scope of forensic readiness goes beyond the IT department's responsibility to become an organizational concern. It also includes more than software, hardware and data; procedures and people are perhaps more important subjects of forensic readiness measures than the technology itself. Forensic readiness actions are not limited to preparation of the system. They have effect in the post-event activities of digital forensic investigations. In addition, these measures are becoming more relevant in assessing the security and risks of the organization and the standing of its stakeholders, not only from a legal perspective, but also from an economic and internal affairs perspective.

Despite this complexity, forensic readiness must be measurable at any point in time in order to be of any use for organizations. Pangalos, Ilioudis & Pagkalos (2010) suggest the need for a forensic readiness metric of the security policies. This is why they describe forensic readiness as "the state of an organisation where certain controls are in place in order to facilitate the digital forensic processes and to assist in the anticipation of unauthorised actions shown to be disruptive to planned operations". It is important to opt for a definitive term for which to develop such a measure.

After realizing the large scope of forensic readiness, as well as the different meanings of similar concepts and the context of the overarching discipline of digital forensics, we can proceed to define the nature of the modern term digital forensic readiness, which is deemed the most appropriate to name the construct of interest in this research.

**Digital Forensic Readiness (DFR)**

Recent papers tend to use the term digital forensic readiness instead of the other terms previously described. DFR is considered a program that "consists of a number of activities that should be chosen and managed with respect to cost constraints and risk" (Reddy, Venter & Olivier 2012), and also "the preparedness of organizations for conducting digital forensics" (Elyas, Maynard, Ahmad & Lonie 2014). These recent papers confirm that DFR is an initial stage of the more complex process of digital forensics. DFR has become so important that the preincident plan for the identification, preservation, and storage of digital evidence is mandatory for UK government offices (Mouhtaropoulos & Li 2012).

Maybe the first practical implementation of DFR policy happened after the HM Revenue and Customs (HMRC) incident on October 18, 2007, when two CDs containing personal information of 25 million individuals and 7.25 million UK families claiming child benefits were missing. The UK government then published the HMG Security Policy Framework (SPF) in May 2010, mandating a Forensic Readiness Policy (FRP) in departments and agencies (Mouhtaropoulos, Grobler, & Li 2011).

Mouhtaropoulos et al. (2011) also say that digital forensics can be proactive or reactive. The proactive digital forensics is the discipline concerned with the achievement of digital forensic readiness. Specifically, there is a clear distinction between digital forensic readiness (DFR) and digital forensics (DF). Digital forensics is a discipline. Digital forensic readiness is a state of preparedness of an organization to obtain, understand, and present digital evidence when needed. DF is to be known and practiced. DFR is to be measured and achieved.

This said, we may be aware that, in both cases, authors use the terms to refer to processes and disciplines. For instance, Farmer & Venema (2005) define computer forensics as the process of gathering and analysing data in a manner as free from distortion or bias as possible to reconstruct data or what has happened in the past on a system (Bem, Feld, Huebner & Bem 2008). Likewise, Fergusson-Boucher & Endicott-Popovski said that network forensic readiness (NFR) has emerged as a method for supporting collection of digital evidence from networks using suggested checklists, procedures, and tools (Fergusson-Boucher & Endicott-Popovski 2012). On the other hand, we found statements such as “digital forensic readiness is a discipline within the field of digital forensics” (Danielsson & Tjøstheim 2004).

Both DF and DFR are associated to other terms, such as risk assessment (e.g. Rowlingson 2004), information assurance (IA) (e.g. Endicott-Popovsky, Frincke & Taylor 2007), IT governance (e.g. Grobler, Louwrens & Von Solms 2010 a and b), and information security (IS) (Hamidovic 2012). This role of DFR in the context of these concepts is not completely clear, although some illustrative contributions are found in the literature. For example, “forensic readiness is complementary to, and an enhancement of, many existing information security activities. It should be part of an information security risk assessment” (Rowlingson 2004); “a forensically ready network incorporates the full spectrum of information assurance (IA) elements: security policies, procedures, practices, mechanisms, and security awareness training programs” (Endicott-Popovsky, Fricke & Taylor 2007); “The accepted literature on digital forensic readiness concentrates mainly on evidence identification, handling and storage, first line incident response and training requirements. It does not consider the proactive application of digital forensic tools to enhance the corporate governance structures (specifically information technology governance)" (Grobler, Louwrens & Von Solms 2010a); and "Digital forensic readiness is a natural progression for organizations with a mature information security posture" (Hamidovic 2012). Given the importance of these concepts in the organizational sciences, the following section elaborates on the role of DFR in the framework of these information security elements.

### Role of DFR in the Organization

Information security (IS) is, as DFR, a state; in this case, the state of security of an organization or a system. Substantial development on the actions leading to better levels of information security has allowed us to see IS as a process, as well. "Information security can be defined as the process of protecting information and information assets from a wide range of threats in order to ensure business continuity, minimize business damage, maximize return on investments and business opportunities by preserving confidentiality, integrity and availability of information" (Taylor, Endicott-Popovsky & Frincke 2007).

IS is also considered a discipline, due to not only the vastness of academic production on the topic, but also due to its increasing importance in the organizations' corporate governance. "Information security governance is an integral part of corporate governance, and consists of the management and leadership commitment of the board and top management towards good information security, the proper organizational structures for enforcing good information security, full user awareness and commitment towards good information security, and the necessary policies, procedures, processes, technologies and compliance enforcement mechanisms all working together to ensure that the confidentiality, integrity and availability (CIA) of the company's electronic assets (data, information, software, hardware, people etc.) are maintained at all times" (VonSolms 2006).

Corporate governance, within which IS governance is embedded, is defined by Elachgar, Boulafdour, Makoudi & Regragui (2012) as all taken responsibilities and practices implemented by a general direction in order to provide a strategic direction and ensure objectives are met, risks are managed appropriately, and organizational resources used responsibly.

Grobler, Louwrens & Von Solms (2010a) see governance as one of the dimensions of digital forensics along with people, policies, laws, processes and technology. Other authors propose DFR as a step beyond IS: “digital forensic readiness is a natural progression for organizations with a mature information security posture, enabling them to pursue perpetrators in the legal domain when other security measures have failed” (Danielsson & Tjøstheim 2004; Hamidovic 2012). Likewise, a focus group of experts suggested that “DFR supports the information security program by enhancing the security posture and deterring potential attackers” (Elyas et al. 2015). Valjarevic & Venter (2011) “believe that DFR should be a built-in security feature and not merely an add-on”.

Maconachy, Schou, Ragsdale & Welch (2001) contend that information systems security (INFOSEC) has evolved into information assurance (IA) and that IA encompasses IS. Hamidovic also shows a strong connection between information assurance and DFR. He contends that the organization's forensic readiness ca be assessed based on criteria suggested by the UK Information Assurance Advisory Council (IAAC): 1) the main likely threats it faces; 2) what sorts of evidence it is likely to need in a civil litigation or criminal proceeding and how it will secure that data; 3) the amount and quality of evidence it has collected; 4) knowledge of the potential legal problems such as admissibility, data protection, human rights, limits to surveillance, obligations to staff members and disclosure in legal proceedings; and 5) the management, skill, resource implications and action plan (Hamidovic 2012).

Despite the above suggested connections among DF, DFR, information security and other concepts, there is not a widely accepted framework to assess DFR. “Digital forensic readiness is often ad hoc and no consistent application or framework exists globally” (Mouhtaropoulos, Grobler & Li 2011). In part, this is due to the lack of clarity on the nature of these concepts when put together in a conceptual model. Some of them are processes, some are states or stages, others are disciplines, and some are several of them simultaneously. Therefore, the proposed frameworks might be seen differently according to the reader’s perspective.

One way to start visualizing the framework of DFR is by using a common unit among the elements in the model. For that reason, the present paper proposes a comparison of the previously explored concepts in terms of the tasks associated to them.

Giiven that the tasks necessary to achieve DFR are the initial step in the complete DF investigation process they must be a subset of the DF tasks. On the other hand, all the tasks of the IS program are part of the global corporate governance activities. Likewise, the tasks in DF investigations and DFR programs are part of the corporate governance. “DFR allows organizations demonstrate due diligence for good corporate governance” [Grobler & Louwrens 2007]. Von Solms & Louwrens (2007) show how IS and DF overlap (Table 1, p. 16) and how IS and DFR overlap (p. 20). “Whilst information security and DF are considered as two different disciplines, there is a definite overlap between the two” (Von Solms & Louwrens as cited by Grobler & Louwrens 2007).

However, despite the considerable overlap between IS and DRF, not all DFR-related tasks belong to the IS strategy. “Information security programmes often focus on prevention and detection measures. From a preventative information security perspective, there is little need for digital evidence” Rowlingson (2004). Tan, Ruighaver & Ahmad (2003) say that “in any computer security incident there will be a tendency to focus on containment and recovery, as these are the foremost business critical issues. However, in stressing these, any evidence that might be required may be damaged, discarded or simply ignored” (Tan et al. 2003 as cited by Rowlingson 2004). Moreover, high levels of DFR provide benefits beyond being the source of evidence for IS-related events. DFR allows organizations demonstrate due diligence for good corporate governance (Grobler & Louwrens 2007).

In fact, the objective of achieving high levels of IS and DFR can be contradictory endeavors. IS concentrates on confidentiality, integrity, and availability (CIA), but not on the preservation of evidence, as DFR does (Pangalos, Ilioudis & Pagkalos 2010). This means that some tasks, such as disconnecting a hacked device from a network may be recommended by the organization’s IS protocol while contrary to the DFR program. This is similar to the work of the police officer versus the work of the journalist. While the officer wants to stop the crime as soon as possible, the journalist tries to find the right angle to capture the complete video of it. Likewise, while Information security aims to eliminate vulnerabilities to eventual attacks, DFR takes advantage of these vulnerabilities to collect as much evidence as possible from the attacks. Forrester & Irwin (2007) assert that unlike the police, businesses use the approach of the military, which requires identification of the incident, and propose mechanisms to deal with both the military and the police approaches in parallel by using forensic readiness.

Privacy, an important asset of IS, also goes in contradiction with DFR. “privacy concerns are a “showstopper” for the deployment of digital forensic readiness” (Danielsson & Tjøstheim 2004). Only corporate governance may be able to reconcile these differences in some organizations. These set of relationships among the activities of DFR, DF, IS and corporate governance can be represented by the following model in figure 1:

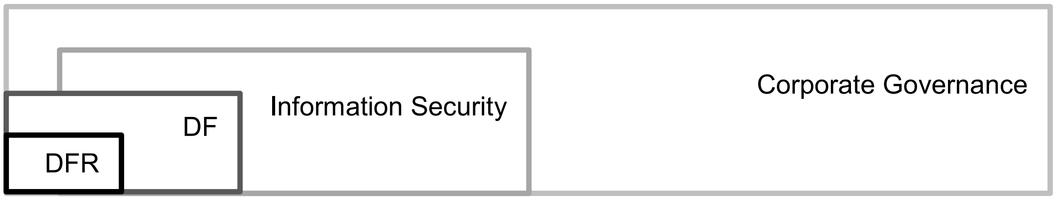


Figure 1. Venn Diagram - The context of DFR tasks

Since the purpose of this research is to advance in finding a unified framework allowing the measurement of DFR, we require understanding of the role of DFR in the organization, but also of the goals, dimensions, activities and factors associated to DFR. The following section explores the literature in relation to these aspects.

### Digital Forensic Readiness Goals

Forensic readiness was from the very beginning defined in terms of its goals:

1. Maximizing the environment’s ability to collect credible digital evidence, and
2. Minimizing the cost of forensic during an incident response (Tan 2001)

Mouton & Venter (2011), interpreting Tan, assert that DFR is put in place to:

1. Decrease the time period required to perform a digital forensic investigation
2. Reduce the cost involved in performing a digital forensic investigation
3. Maximize the ability to collect the evidence without disrupting the environment

Elyas, Maynard, Ahmad & Lonie (2014) recognize that the goals of DFR can be diverse. They express them in the form of three capabilities that a forensically ready organization must have:

1. To produce evidence that facilitates the demonstration of regulatory compliance

2. To produce evidence to facilitate internal investigations

3. To produce evidence that can be used in legal proceedings (legal evidence management)

In addition, Rowlingson (2004) says that this preparation can also be a deterrent for internal crimes. Likewise, Danielsson & Tjøstheim (2004) say that the management of digital evidence is a means to limit business risk, and compare the DFR measures with those that "organizations take in the physical world to monitor their buildings with, for example, video surveillance (i.e. CCTV), guards, and by logging information about all persons that enter and leave their office buildings". The collection and preservation of digital evidence would limit business risk by providing support for:

1. Legal defense
2. Civil litigation
3. Criminal prosecution
4. Internal disciplinary actions
5. Claim to intellectual property
6. The documentation of due care
7. The documentation of the impact of a crime or disputed action in order to support an insurance claim or a claim for damages (Danielsson & Tjøstheim 2004)

They say that these measures serve 3 interdependent purposes:

1. Provide a deterrent effect

2. Support the detection of suspicious events

3, Provide support in answering the questions post mortem of who, when, how and what

Although, they acknowledge DFR support of the recovery process, its focus, according to them, is on the third purpose of providing information about transpired events.

According to this diversity of purposes one question that researchers and practitioners should answer before assessing the forensic readiness of organizations is: ready for what? A review of the literature leads us to different approaches.

Carrier & Spafford (2003) say that this is an ongoing phase whose goal "is to ensure that the operations and infrastructure are able to fully support an investigation. Both digital and physical evidence can be lost if it is not maintained and collected properly" (Carrier & Spafford 2003). This statement highlights the infrastructure and operations dimensions and opens the domain of DFR not only to the digital, but also to the physical evidence.

Other factors and dimensions can be identified from other authors. Factors such as cost, business continuity, and benefit/cost proportionality can be inferred from Rowlingson's (2004) proposed goals of DFR, which are adopted in posterior research (e.g. Pangalos, Ilioudis & Pagkalos 2010):

1. To gather admissible evidence legally and without interfering with business processes
2. To gather evidence targeting the potential crimes and disputes that may adversely impact an organization
3. To allow an investigation to proceed at a cost in proportion to the incident
4. To minimise interruption to the business from any investigation
5. To ensure that evidence makes a positive impact on the outcome of any legal action (Rowlingson, 2004)

For Rowlingson, DFR is itself a corporate goal that involves technical and non-technical actions that maximize the ability of an enterprise to use digital evidence (Reddy & Venter 2009).

Grobler, Louwrens & Von Solms (2010 a and b) use the term Proactive Digital Forensics (ProDF) for which they propose the following goals:

1. Become DF ready
2. Enhance the Governance programs (IT and IS of the organization by proving (assessing) the effectiveness of controls, measured against IT and IS objectives related to business objectives)
3. Improve IS / IT performance with the responsible use of DF tools to improve effectiveness and efficiency in organization (Grobler, Louwrens & Von Solms 2010 a and b).

Pangalos, Ilioudis & Pagkalos (2010) say that forensic practices are “departing fast from the niche of law enforcement and becoming a business function and infrastructural component.” One example of this happened to Target in 2014. According to the expert Steve Durbin, Target attack was done through exploiting a web service application used by a HVAC vendor to supply invoices (Olavsrud 2015). “From Target to Sony the number of breaches continues to increase affecting also employees and customers” (Starkman 2014). This leads us to propose that another objective of DFR would be to demonstrate good practices to suppliers and customers.

An observation from this analysis is that the objectives of DFR might be identifiable according to the interested party involved, which may also give an idea of the DFR status of the firm. A radial chart can be used to show this coverage of stakeholders according to the DFR objectives. In general, companies must be able to demonstrate regulatory compliance through the formalization of procedures and the commitment of managers and members of the board. One step further includes control its own environment, including employees' behavior and daily interactions with customers. This will prepare the organization to conduct internal investigations. Commercial disputes will require this internal control, as well as control over the interactions with other companies, such as suppliers and partners. Finally, these internal and external controls might not be enough for the firm to deal with unknown interested third parties, such as anonymous cyber-criminals or digital bunglers. Dealing with this requires more than having good policies and procedures, internal and external controls in place, and complying with regulations. It requires up to date knowledge of threats, vulnerabilities and safeguards and sophisticated methods and personnel to perform intelligence. At this level, interested parties easily include judiciary and executive authorities, and foreign companies and governments. In general, the farther a stakeholder is from the center of the circle the more challenging it is for the organization to deal with DFR goals associated to that stakeholder.

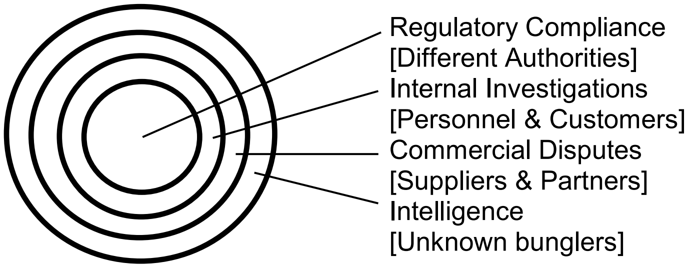


Figure 2. Goals Coverage of DFR

The radial scope of this chart does not necessarily imply that organizations achieve higher levels of DFR from the center outward. Casey (2005) gives an example of an intrusion difficult to track because the organization only had monitoring systems on the internet border, but not on its internal subnets. Which are the activities of DFR aiming to achieve its goals is the subject of the next section.

### Digital Forensic Readiness Activities

There are different approaches in understanding the several activities involved in the process of gaining DFR. Carrier & Spafford divide them in operational and infrastructure. “The operations readiness phase provides training and equipment for the personnel that will be involved with the incident and its investigation. This includes training the responders, the lab analysts, and staff that will be receiving the initial reports of the incident. The infrastructure readiness phase ensures that the needed data exists for a full investigation to occur. After all, it is difficult to analyze data if it does not exist. This phase only applies to those who maintain the environment that could be the target of a crime (Carrier and Spafford 2003). In addition, they explain that infrastructure can be physical or digital. Cameras and card readers are examples of the physical phase. Examples of the digital phase include sending server logs to a secured log host, synchronizing the internal clocks on servers with network time protocol (NTP), creating a baseline of MD5 hashes, and maintaining a change management database.

The key activities in implementing a forensic readiness programme for Rowlingson (2004) are:

1. Define the business scenarios that require digital evidence
2. Identify available sources and different types of potential evidence
3. Determine the evidence collection requirement
4. Establish a capability for securely gathering legally admissible evidence to meet the requirement
5. Establish a policy for secure storage and handling of potential evidence
6. Ensure monitoring is targeted to detect and deter major incidents
7. Specify circumstances when escalation to a full formal investigation (which may use the digital evidence) should be launched
8. Train staff in incident awareness, so that all those involved understand their role in the digital evidence process and the legal sensitivities of evidence
9. Document an evidence-based case describing the incident and its impact
10. Ensure legal review to facilitate action in response to the incident

Although policies are seen as a specific dimension of DFR, Taylor, Endicott-Popovsky & Frincke (2007) offer steps to define the forensics policy addressing forensic readiness for a given system:

1. Identify digital assets that have value

2. Perform a risk assessment for potential loss and threat to those assets

3. Remove assets that do not warrant the effort of prosecution

4. Identify associated data needed for these assets along with collection and storage needs

5. Write the forensic policy in terms of digital assets, forensic events, data collection and storage

6. Ensure adequate forensics policy enforcement is in place.

A structured approach in digital forensic readiness, according to Danielsson & Tjøstheim (2004), should at least include:

1. An analysis of legal requirements and constraints on collection and preservation of potential digital evidence in the applicable legal context

2. A method for analyzing the organizations' need for digital evidence

3. An identification and classification of potential digital evidence sources, and enumeration of technologies and processes for utilizing these sources

4. Guidelines for preserving digital evidence, including processes, procedures, and suggestions as to how technology solutions can be used

5. Guidance on when and how to report incidents to the law enforcement, including content and formats of reports, criteria for reporting, and standardization of the interaction between affected parties and law enforcement

Grobler et al. (2010a) decompose the process of becoming forensic ready into steps as follows:

1. Provide and prepare the infrastructure to support DF investigations

2. Develop an evidence management plan (EMP) including an evidence map and evidence management policies and procedures to manage CDE

3. Augment organizational risk mitigation plans to include evidence and process requirements. Apply an algorithm to calculate the completeness and admissibility of the evidence. Implement an Intrusion Detection System (IDS). Define trigger events for investigations. Prepare for containments of incidents to include containment on live systems

4. Develop a DF training and awareness strategy with training and awareness programmes for the organization

5. Develop a management capability to outline the internal and external DF investigators and the role and responsibilities of the Computer Emergency Response Team (CERT)

6. Document and validate a DF investigation (DFI) protocol (Active and Reactive) against best practice

7. Establish procedures and policies to ensure that an investigation proceed at a cost in proportion to the incident

8. Minimize interruption to the business from any investigation

**Factors Affecting Digital Forensic Readiness**

One of the earliest approaches to determine the status of DFR in organizations can be extracted from Yasinsac & Manzano (2001). They propose a set of computer and network policies to deter computer crime and enhance computer forensics, which are some of the cited goals of DFR. Given that the factors of interest are conditions that might determine the state of DFR in an organization we can turn Yasinsac & Manzano's policies into questions in order to assess their impact. For example:

A. Retaining Information

A1. Does the organization copy and retain application and local user files?

A2. Does the organization copy and retain computer and network activity logs?

B. Planning the response

B1. Does the organization have a forensic team?

B2. Does the organization have an intrusion response procedure?

B3. Is there a formal investigative procedure?

C. Training

C1. Is there training for the response team?

C2. Is there training for the investigative team?

C3. Is there training on DF for all personnel that use computers?

D. Accelerating the investigation

D1. Is personal file encryption prohibited?

D2. Is disk scrubbing tools and file shredding software prohibited?

D3. Are data indexes utilized?

D4. Is information fusion utilized?

E. Prevent anonymous activities

E1. Is onion routing prevented or used?

E2. Are date, time and user stamps in file required?

E3. Is strong user authentication used?

E4. Are strong access control mechanisms used?

F. Protect the evidence

F1. Is there rigid control over administrative access for systems housing potential evidence?

F2. Are evidence files and connections encrypted?

F3. Is there strong integrity checking technology? (Adapted from Yasinsac & Manzano 2001).

Yasinsac & Manzano's six categories of policies have been retaken by later authors (e.g., Rowlingson 2004; Pooe & Labuschagne 2012), and is a starting point to identify how different factors can be grouped into different dimensions. However, because DFR is part of DF, the dimensions of DF must also be considered in order to propose the dimensions of DFR. Grobler et al. (2010a) propose a model in which the dimensions of digital forensics are:

1. Legal (which deals with compliance). The legal and judiciary dimension is the backdrop for the digital forensic management framework (DFMF) as it will influence all the activities of the organization
2. Governance (Management of facilities, partners, and risk)
3. Policies (answers to the 'what', 'when' and 'who' questions)
4. Process (answers to the 'what', 'when', 'how', 'where' and 'who' questions)
5. People (answers to the 'who' question)
6. Technology (addresses applications and technologies to use)

Although there is a clear advantage in the categorization of factors and the identification of dimensions, several challenges can be seen from these frameworks. On one hand, it is important to identify the relationships among the different dimensions, which not always are comprehensive and independent as to be put in a statistical analysis of principal components. This is evident based on the statement "the governance dimension is a subset of the legal and judiciary dimension. The other dimensions people, policy, process and technology are subsets of the Governance dimension" (Grobler, Louwrens & Von Solms 2010).

On the other hand, the dimensional approach can have several layers with relationships among factors and dimensions crossing through those different levels. For example, from the two previous categorizations we can see that Yasinsac & Manzano's categories of policies are set in the form of processes, which puts them into the process dimension of Grobler et al.'s (2010a) framework. However, training is a process directed to people. Therefore, the training policies of Yasinsac & Manzano are also closely related to the people dimension of Grobler et al., and both, then, are related to the governance and legal dimensions, which are one and two levels above respectively, according to Grobler et al. (2010a).

To top it off, one single category in Yasinsac & Manzano's framework can demand several indicators in order to be assessed appropriately. Let us take the category "retaining information" for example. Basic questions about possible source of evidence to be retained are given by Rowlingson (2004):

1. Where is data generated?
2. What format is it in?
3. For how long is it stored?
4. How is it currently controlled, secured and managed?
5. Who has access to the data?
6. How much is produced?
7. Is it archived? If so where and for how long?
8. How much is reviewed?
9. What additional evidence sources could be enabled?
10. Who is responsible for this data?
11. Who is the formal owner of the data?
12. How could it be made available to an investigation?
13. To what business processes does it relate?
14. Does it contain personal information?

Stephenson (2003) uses a similar set of questions to summarize what he considers factors affecting the digital investigation, but in this case his focus is in the incident:

1. What is the nature of the incident?

2. How can we be sure that there even was an incident?

3. What was the entry point into the target system? Was there only one?

4. What would evidence of an attack look like? What are we looking for?

5. What legal issues need to be addressed (policies, privacy, subpoenas, warrants, etc.)?

6. Who was in a position to cause/allow the incident to occur?

7. What security measures were in place at the time of the incident?

8. What non-technical (business) issues may have impacted the success or failure of the attack?

9. Who knew what about the attack and when did they know it? (Stephenson 2003).

In fact, the closest substitute for a DFR framework can be found in proposed frameworks for the digital investigation process. Stephenson used the DFRWS Digital Investigation Framework to elaborate his End-to-End Digital Investigation (EEDI) technique. This framework as cited by Reith, Carr & Gunch (2002) comprises 7 stages, whereas Stephenson talks about 6 classes. Although, the framework is essentially the same, the present research pays special attention to the terminology used in the literature in order to propose a standard framework of DFR. Therefore, the elements of the DFRWS framework are included as candidate factors or dimensions of DFR and submitted to later classification following the methodology adopted here. These elements are:

A. Identification

A1. Event/Crime Detection

A2. Resolve Signature

A3. Profile Detection

A4. Anomalous Detection

A5. Complaints

A6. System

A7. Monitoring Audit Analysis

B. Preservation

B1. Case Management

B2. Imaging Technologies

B3. Chain of Custody

B4. Time Synchronization

C. Collection

C1. Preservation

C2. Approved Methods

C3. Approved Software

C4.Approved Hardware

C5. Legal Authority

C6. Lossless Compression

C7. Sampling

C8. Data Reduction Recovery

C9. Recovery Techniques

D. Examination

D1. Preservation

D2. Traceability

D3. Validation Techniques

D4. Filtering Techniques

D5. Pattern Matching

D6. Hidden Data Discovery

D7. Hidden Data Extraction

E. Analysis

E1. Preservation

E2. Traceability

E3. Statistical

E4. Protocols

E5. Data Mining

E6. Timeline

E7. Link

E8. Spatial

F. Presentation

F1. Documentation

F2. Expert Testimony

F3. Clarification

F4. Mission Impact Statement

F5. Recommended Countermeasure

F6. Statistical Interpretation (DFRWS cited by Stephenson 2003)

Carrier & Spafford (2003) noted ambiguity in the distinction of the preservation and collection phases, and the analysis and examination phases. Thus, they propose their own framework consisting of five groups of phases:

1. Readiness

2. Deployment

3. Physical crime scene investigation

4. Digital crime scene investigation

5. Presentation

Other models of the digital investigation process can be found in Casey (2000) (1. Recognition, 2. Preservation, collection, and documentation, 3. Classification, comparison, and individualization, and 4. Reconstruction) and Lee 's (2001) Model of Scientific Crime Scene Investigation (1. Recognition, 2. Identification, 3. Individualization, 4. Reconstruction) (Ciardhuáin 2004). For the purpose of this research, items such as preservation, which in Stephenson (2003) framework is present in several classes, or spatial, which looks like a dimension itself rather than a factor, represent a challenge of classification (These issues are addressed in the section of methodology). A more manageable set of factors come in the form of questions.

From Kent, Chevalier, Grance & Dang (2006) Guide to Integrating Forensic Techniques into Incident Response, which they developed for the National Institute of Standards and Technology (NIST), we can extract a different set of key questions:

1. What are the potential sources of data?

2. Of the potential sources of data, which are the most likely to contain helpful information and why?

3. Which data source would be checked first and why?

4. Which forensic tools and techniques would most likely be used? Which other tools and techniques might also be used?

5. Which groups and individuals within the organization would probably be involved in the forensic activities?

6. What communications with external parties might occur, if any?

7. From a forensic standpoint, what would be done differently if the scenario had occurred on a different day or at a different time (regular hours versus off-hours)?

8. From a forensic standpoint, what would be done differently if the scenario had occurred at a different physical location (onsite versus offsite)?

Kent et al.. (2006) also highlight the importance of the existence of a toolkit and team response, of clear weighed criteria on whether turning off a hacked device or not, and of clear weighed criteria on volatility orders to collect evidence in each case.

It is not surprising then that, given this plurality of potential factors of DFR with such complex relationships among them, there is not an accepted framework to assess DFR. Instead of a measurement model many authors hence propose policies, requirements, strategies and protocols in order to help organizations to be forensically ready. For example, Endicott-Popovsky, Frincke & Taylor (2007) use four strategies (called the 4R model for resistance, recognition, recovery and redress) to categorize the abilities and tools necessary for network forensic readiness (NFR). These tools and abilities can be considered factors that determine the DFR state. They are:

Resistance

1. Ability to repel attacks using tools such as firewalls, user authentication, and diversification

Recognition

2. Ability to detect an attack or a probe using ids and internal integrity checks

Recovery

3. Ability to provide essential services during attack and restore services following the attack using incident response, replication, backup systems, and fault tolerant design

Redress

4. Ability to hold intruders accountable in a court of law and to retaliate using forensics (the who), legal remedies and active defense

Additionally, two more candidates of factors can be extracted from Endicott-Popovsky et al.'s work:

5. The identification of relevant target assets

6. The test and calibration of the collection devices and their frequency of calibration

Mouhtaropoulos, Grobler & Li (2011) say that a forensic readiness policy (FRP) should consider:

1. Digital evidence (DE) identification
2. Risk Assessment by classifying DE exposure and correlating with threats
3. Control to DE access and maintenance of a digital chain of custody (DCOC)
4. Statistical representation of the DE by establishing a Bayesian network; it will calculate the relationship between cost and benefit factors of each measure
5. The events that will escalate an event into a full forensic investigation; the policy should specifically correlate events with the established Bayesian network
6. Evidence Management Plan development
7. Single point of contact (SPOC) establishment with legal authorities
8. Digital forensic investigation (DFI) model choice - the procedure to be followed after an incident occurs
9. Technical infrastructure standards
10. Staff training procedures on the policy's contents

Barske, Stander & Jordaan (2010) contend that "numerous varying factors such as the perceived high cost, as well as the current lack of forensic skills, make the implementation of digital forensic readiness appear difficult if not infeasible for smaller organisations". They summarize the Components of DFR as:

1. Strategy
2. Compliance & Monitoring
3. Policy & Procedures
4. Technology and Digital Forensic Response

They also identified the following factors that may play a role in the decision of adopting a forensic readiness plan and the level of its implementation:

1. The industry sector (financial institutions may be more likely to adopt a higher level of forensic readiness as they handle financial transactions)
2. The funding available.
3. More employees increase the risk of internal criminal incidents and the need for forensic readiness
4. More staff with access to financial instruments increases the chances of incidents of fraud and the need for forensic readiness
5. Staff with more advanced IT skills in the organization increases the chances of being able to multi-skill some of them to handle forensic cases, which reduces costs of adoption
6. Organizations with public profiles are more likely to adopt forensic readiness to maintain their reputation

Legal requirements, as well, give indications of what factors must be considered in order to be forensic ready. According to Leigh (2012), English courts have an electronic disclosure protocol requesting organizations providing digital evidence (including computer files, mobile phone records, smartphone data, tablet data, electronic booking system records, photographs, voicemail, data back-up tapes) to inform about:

1. IT systems in use
2. Where data is stored
3. Back-up procedures
4. Electronic document retention and archiving policies
5. The number of documents likely to be located (Leigh 2012)

Therefore, these five aspects plus the legal requirement itself can be considered among potential DFR factors. In addition, Leigh underlines the importance of some considerations that could be considered determinants in DFR. For example:

1. Tracing custody of individual PCs, laptops and PDAs for upgrades people's change of office or role
2. Asset registry for items of electronic equipment that could record information
3. Employment law or privacy issues

4. Training in awareness

5. Centralization of data

6. Storage in personal devices (Leigh 2012)

Reddy, Venter & Olivier (2012) explain that the challenge for managers is to coordinate the organisational resources to attain an acceptable level of DFR. Reddy & Venter (2013) developed an architecture for a DFR Management System DFRMS based on basic requirements that the proposed system should accomplish according to the extant literature (Details about the source of Reddy & Venter's requirements can be found in Table 1, p. 76 of their paper). Given that these requirements are proposed as necessary conditions for achieving a good level of DFR, we can treat them as factors in a preliminary exploration. These requirements are:

1. Monitor or log network and host activity

2. Secure storage of logs

3. Intrusion detection system

4. Distinguish whether hardware or software elements are being monitored

5. Automated alarm upon detection of potential or actual incident

6. Configuration procedures for monitoring and logging

7. Investigative teams (DF teams) and incident response teams' descriptions

8. Training requirements and training

9. Business process descriptions

10. Organizational DF policies and policies related to DFR

11. Suspicion policy

12. Law enforcement contact policy

13. Escalation procedure

14. Incident response procedure

15. Law enforcement contact procedure

16. Organizational structure and staff involved in DFR and incident response

They also make a contribution worth considering among potential factors, which is the existence of three types of software related to the management of DFR:

1. Intrusion detection systems (IDS) monitoring events on computers and networks

2. Security event management software (SEM), which filter real threats from false alarms

3. Incident management software, controlling the workflow involved in the incident management process through incident records, escalation rules, information about end users, and about configuration items (Reddy & Venter 2013)

Similarly, an approach based on functionalities contends that a system for DFR in the cloud was deemed to require:

1. Communication Channel

2. Encryption

3. Compression

4. Authentication of log data and proof of integrity

5. Authenticating the client and server

6. Timestamping (Trenwith & Venter 2013)

Finally, Elyas, Maynard, Ahmad & Lonie (2014) propose eleven factors:

1. Forensic strategy

2. Non-technical stakeholders

3. Technical stakeholders

4. Technology

5. Monitoring

6. Architecture

7. Policy

8. Training

9. Forensic culture

10. Top management support

11. Governance

These same authors later changed the denomination of “factors” by the term “capabilities” in a follow up of their framework performed with focus groups of DF experts (Elyas, Ahmad, Maynard & Lonie 2015). In their new study, they introduced different perspectives from which DFR has been studied:

1. Resourcing (e.g. Reyes & Wiles, 2007)

2. Technology use and selection (e.g. Carrier & Spafford, 2003)

3. Training (e.g. Carrier & Spafford, 2003; Rowlingson, 2004)

4. Legal investigations (e.g. Casey, 2005)

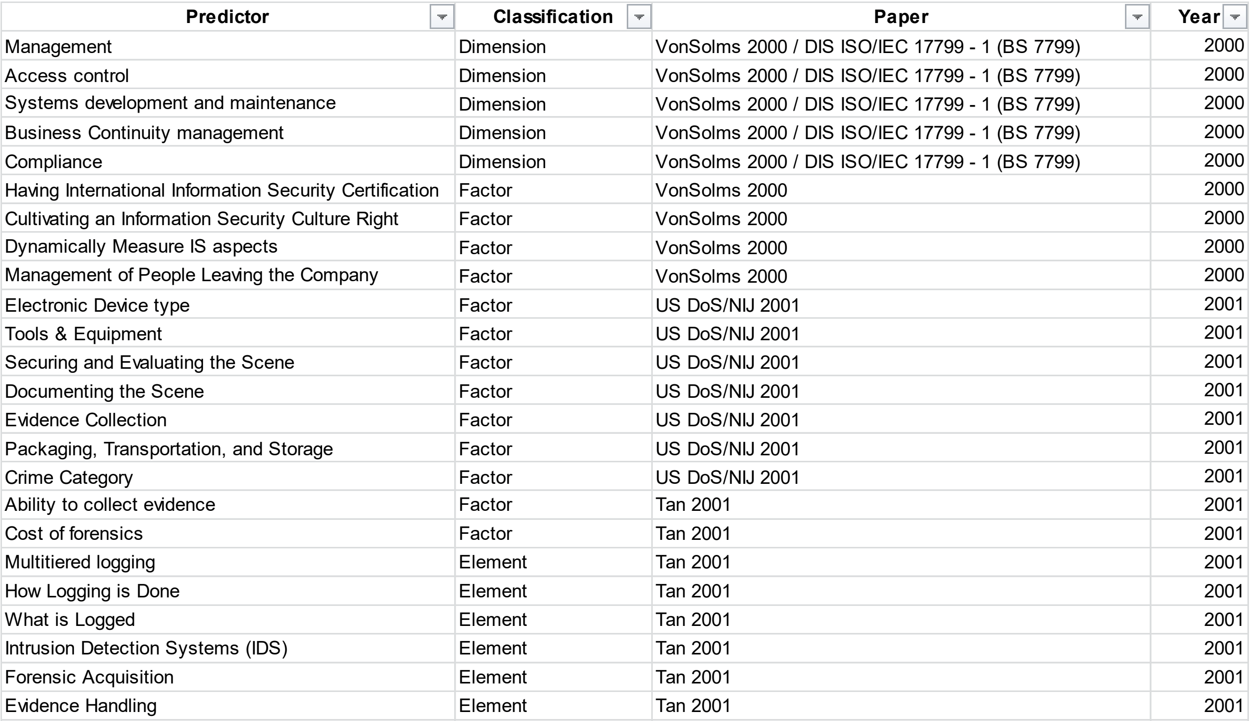
5. Incident response (e.g. Ahmad et al.., 2012; Shedden et al.., 2010a; Tan et al.., 2003)

6. Policy (e.g. Yasinsac & Manzano, 2001)

All these factors must be considered in the analysis of the DFR framework. However, in this paper, a factor will be treated as a condition, something that is present to a specific extent and can be the cause of something else: “a phenomenon presumed to affect an experiment” (Wikipedia 2015). For this reason, some of the factors previously listed are better seen as dimensions in the way this term is used in the social sciences. A dimension is something that is characteristic of the subject or a perspective from which that subject can be seen. “A dimension is a structure that categorizes facts and measures in order to enable users to answer business questions … Perhaps the most basic way the word dimension is used in literature is as a hyperbolic synonym for feature, attribute, aspect or magnitude” (Wikipedia 2015).

According to this, we cannot, for example, use governance as a factor. Governance could be a dimension. The factor would be to what extent there is governance or to what extent governance includes IT policies. This paper’s objective is to find factors that are measurable with scales that vary from low to high. These factors, nevertheless, can be grouped in dimensions in order to facilitate the comprehension and analysis of the problem. For this reason, the previous literature review on factors, dimensions, activities, and goals related to DFR are of paramount importance in the final definition of the usable factors for this paper. The work of these researchers, regardless of the terminology used, unveils many relevant measurable indicators of the extent to what DFR is achieved in an organization.

A partial view of the preliminary list of potential factors and dimensions found in the literature is presented below. This list considers not only what has been explicitly mentioned by the authors, but also what could be inferred from their contentions. Therefore, some items in the list are presented as in the original, while some others have been reworded or redacted for the first time. The complete list of 1115 items is too large to include in the body of this paper, but it is provided as Appendix A.



| Predictor | Classification | Paper | Year |
|---|---|---|---|
| Management | Dimension | VonSolms 2000 / DIS ISO/IEC 17799 - 1 (BS 7799) | 2000 |
| Access control | Dimension | VonSolms 2000 / DIS ISO/IEC 17799 - 1 (BS 7799) | 2000 |
| Systems development and maintenance | Dimension | VonSolms 2000 / DIS ISO/IEC 17799 - 1 (BS 7799) | 2000 |
| Business Continuity management | Dimension | VonSolms 2000 / DIS ISO/IEC 17799 - 1 (BS 7799) | 2000 |
| Compliance | Dimension | VonSolms 2000 / DIS ISO/IEC 17799 - 1 (BS 7799) | 2000 |
| Having International Information Security Certification | Factor | VonSolms 2000 | 2000 |
| Cultivating an Information Security Culture Right | Factor | VonSolms 2000 | 2000 |
| Dynamically Measure IS aspects | Factor | VonSolms 2000 | 2000 |
| Management of People Leaving the Company | Factor | VonSolms 2000 | 2000 |
| Electronic Device type | Factor | US DoS/NIJ 2001 | 2001 |
| Tools & Equipment | Factor | US DoS/NIJ 2001 | 2001 |
| Securing and Evaluating the Scene | Factor | US DoS/NIJ 2001 | 2001 |
| Documenting the Scene | Factor | US DoS/NIJ 2001 | 2001 |
| Evidence Collection | Factor | US DoS/NIJ 2001 | 2001 |
| Packaging, Transportation, and Storage | Factor | US DoS/NIJ 2001 | 2001 |
| Crime Category | Factor | US DoS/NIJ 2001 | 2001 |
| Ability to collect evidence | Factor | Tan 2001 | 2001 |
| Cost of forensics | Factor | Tan 2001 | 2001 |
| Multitiered logging | Element | Tan 2001 | 2001 |
| How Logging is Done | Element | Tan 2001 | 2001 |
| What is Logged | Element | Tan 2001 | 2001 |
| Intrusion Detection Systems (IDS) | Element | Tan 2001 | 2001 |
| Forensic Acquisition | Element | Tan 2001 | 2001 |
| Evidence Handling | Element | Tan 2001 | 2001 |

Figure 3. Preliminary Factors and Dimensions of DFR (Partial View)

Clearly, some of these factors and dimensions show up repeatedly in different works, some are mentioned by other authors not presented in the list, and others may not be in the list. This list does not pretend to present the factors in a specific order or imply that a factor listed was proposed originally by the article from where it was extracted. The list's main purpose is to be as inclusive as possible from the literature reviewed. Many of the factors included are indeed recurrent throughout the literature of digital forensics.

This is only a preliminary step in the search for the final factors that might be affecting how an organization moves towards a specific status of DFR. The next section explains the structured process used to find the factors affecting DFR.

# CHAPTER III

# METHODOLOGY

Although DFR is being practiced and studied more every day, the literature and practitioners have not yet reached an agreement on a common framework to assess DFR and implement measures to improve it. A diversity of methodologies exists for the implementation of DFR and several distinct factors can affect its status according to different objectives.

This dissertation proposes a strategy that combines the review of the extant literature, the views of other qualified reviewers and the answers from professionals working on IT security in order to obtain a comprehensive framework of the factors that determine DFR. Both qualitative and quantitative techniques are applied in the process of extracting the knowledge from primary and secondary sources of data.

This research shows that there is great diversity and amount of potential factors of DFR. The challenge lies in identifying and classifying a complete and succinct set of those factors which can explain the DFR status in organizations. Complete means that the DFR framework should include as many factors as possible that explain variation in DFR status. Succinct means that only those factors which capture variance of the DFR not explained by other factors should remain in the framework.

In order to be as complete as possible, this research extracts all potential indicators identifiable in the DFR literature available. These indicators can be factors in their own right or be a lower level of a factor in conjunction with other indicators. These factors and the relationship among them is what constitute the resulting model of DFR. In addition, dimensions should be identified such that professional practitioners, who may not be familiar with concepts such as latent variables and conceptual models, can, nevertheless identify the aspects of the organization that the factors represent.

The terms factor and indicator are use indistinctly in parts of this work because they both are indications or predictors of the level of certain condition, DFR in this case. They both can be variables in a statistical model. When the factor can be subdivided in more specific lower level factors we talk about indicators. It is important to understand also that factors affecting a construct cannot be assessed unless there is a measure of the construct to which to compare the impact of the variation of the factors. Because that measure of DFR does not exist, this research proposes it and identifies the factors affecting it. The way this is done is by distinguishing between extant and perceptual factors and then comparing their relationship.

As academics, we should expect that researchers proposing frameworks, methodologies and assessments of DFR are accounting for all what they consider affects its status. Therefore, a literature review should provide a comprehensive set of indicators of DFR. Of those indicators, some refer to elements that the organization has, knowledge that it possesses, and actions that it does, and by having them, knowing them, and performing them it enhances its digital forensics preparation. These can be understood as extant DFR indicators because they represent the reality of the DFR status of the firm. On the other hand, there are elements for which no direct verification is available; thus, we search for perceptions, opinions, and attitudes in order to obtain some measure of their presence. These are called perceptual indicators in this research. It is hypothesized here that perceptual factors reflect the DFR status assessed by the extant ones.

This research follows a process divided in two phases in order to develop and test a framework for the assessment of DFR in organizations:

Phase 1: Elaboration of a practical framework through quantitative literature analysis

1. Definition of the research question and identification of the dependent variable
2. Systematic revision of the extant literature in DFR
3. Collection and classification of the DFR indicators extracted from the literature
4. Testing of the dimensional classification through a Q-Sort test
5. Adjustment of the validity of the dimensional classification using association rules

Phase 2: Elaboration and testing of an instrument to assess DFR

6. Refinement of indicators to be used to survey organizations
7. Distinction between extant and perceptual indicators of DFR
8. Assessment of reliability and validity
9. Final survey and exploratory factor analysis

10. Drawing of conclusions, assumptions, limitations and contributions of the study

A detailed description of these stages is elaborated below:

### Phase 1: Elaboration of a Practical Framework through Quantitative Literature Analysis

1. Definition of the research question and identification of the dependent variable

The research question of this study is whether a framework for the assessment of DFR can be found and what the factors affecting DFR in organizations would be. Therefore, the dependent variable of interest is DFR.

As any other variable, DFR can assume different values representing the DFR status of an organization at different moments in time. There is, currently, not a standard measure of DFR against which to develop tests to see how it changes when other variables change. On the contrary, DFR is yet to be comprehensively understood. In fact, it seems like determining the DFR level of an organization will be an unachievable task. How prepared is the organization to respond to a situation requiring digital evidence cannot be known with certainty until such situation happens, which is not a moment firms are longing for. If the situation, though, arises, it can come in many different fashions, and it is unlikely that it will be the same or similar to any other event in the same or a different company. Comparisons, then, are impossible.

Regardless of these difficulties, the need to assess this digital forensic preparedness is real and growing. It is required that researchers minimize uncertainty on the assessment of DFR as much as possible. Given that the DFR indicator does not exist and that no variables can be tested against it (and because of this), this paper is in the quest for finding the factors comprised by the DFR construct.

After reviewing the literature, it becomes clear that many and varied factors complement each other to create the idea of a specific status in terms of DFR in an organization. It is also clear that some factors contribute to the DFR status in a way that is out of the domain of other factors. This indicates that many factors in question are formative rather than reflective. Therefore, finding these factors is, at the same time, understanding the composition of the construct and developing a measure for it that has not been proposed heretofore.

Because many distinct and overlapping factors have been proposed to affect DFR, it is difficult to understand what their prorated unique contributions are. For this reason, this paper proposes a preliminary framework for the classification of the factors found and exposes the indicators of this framework to statistical tests of exploratory factor analysis.

2. Systematic revision of the extant literature in DFR

In the process of developing measures, which is the purpose of this paper, Churchill (1989) recommends to start with specifying the domain of the construct. Likewise, the present paper has begun with a detailed review of the extant literature on DFR in order to recognize the domain and scope of the construct.

The amount of literature on DFR until Decemeber, 2015, is still moderate, especially considering papers published in indexed academic journals. For this reason, this research attempts to review all extant literature whose main topic is DFR frameworks, components, factors or similar aiming to describe how is DFR composed and what factors determine its status. This includes similar terms such as pre-incident preparation (Mandia, Prosise & Pepe cited by Valjarevic & Venter 2011), operation readiness phase and infrastructure readiness phase, (Carrier and Spafford cited by Valjarevic & Venter 2011), proactive digital forensics (Alharbi, Weber-Jahnke & Traore  2011; Mouhtaropoulos Li & Grobler 2012), network forensic readiness, and forensic readiness in the cloud (Ferguson-Boucher & Endicott-Popovsky 2012; Sibiya, Venter & Ngobeni 2013; and Trenwith & Venter 2013). Other papers are included as deemed relevant by citations of the most directly related papers from indexed academic journals.

In the process of this research, 77 DFR-related documents have been examined. Two main sources have been used to limit the scope of the search. One is the library system of a southern university in the United States classified as a highest research institution by the Carnegie classification of institutions of higher education. This includes those volumes available through interlibrary loan service. The second source is the Google Scholar web search engine. The university's library provides access to over 140 databases and 27.000 electronic journals, while Google Scholar database allows access to an estimated of more than 160 million documents including such recognized sources as Elsevier journals.

3. Collection and classification of the DFR indicators extracted from the literature

During this process, the complete selection of papers is reviewed to extract explicit nomination of factors by the authors. Other factors that are inferred from the explanations of the authors are also considered. Each item is initially classified as a factor, dimension, requirement, step, etc., as proposed by the paper’s author(s), and later reclassified as only a factor or a dimension according to the definitions proposed in this research. As explained above, there is no clear and broadly accepted distinction between factors and dimensions throughout the DFR literature. Authors talk about factors, elements, categories, phases, requirements, etc. in ways that are coherent within their own discourse, but difficult to reconcile with each other and to quantify in a comprehensive model. This is also an obstacle in the quest to establish a structured general framework of DFR.

Despite the diversity of proposals, the raw list includes all factors, elements, categories, requirements, etc. as originally mentioned by the authors. From this point on, they will be called items or indicators, and can be part of factors or dimensions or remain as simple indicators. This inclusion of explicit and implicit items helps recognizing different dimensions of the DFR construct according to the literature. Furthermore, by putting all the items on the table, this research minimizes the possibility that any relevant indicator of DFR is left out of consideration, and that any factor or dimension, that surges with the support of that indicator, is dismissed.

One first obstacle is that this comprehensive approach leaves too many potential indicators with no inferable structure. Therefore, some preliminary organization must be done on this list in order to distill a unique categorized set of relevant indicators. Two preliminary operations are conducted on the raw list: reclassification of items as factors or dimensions and elimination of redundant items.

First, all the items are reclassified as potential dimensions or potential factors, which may change the initial denomination by authors as factors, elements, categories, requirements, etc. It was explained before that all those items that can be expressed and seen as potential generators of a specific DFR status are considered factors, whereas those items referring to a perspective or category, within which more granular indicators can be grouped, are considered dimensions.

Factors are more specific than dimensions. They indicate conditions or choices or actions. Although a single factor can be measured through two or more indicators, when several of those conditions, choices or actions are needed to define the item, it may be better deemed as a dimension. For the purpose of this research the factor has to be measurable through variables assuming values on a continuum (e.g. time of experience of the CIO) or at levels/categories (e.g. industry, number of employees by ranges) or, at least, as a binary variable (e.g. have/have not security policy). The description of the factor may also include a verb, such as “support from management”, which indicates that such action, the support, takes place or is performed to some level.

Many items included are questions that authors suggest to ask in order to assess preparedness. An observation from the review is that, in general, questions such as “how much”, “for how long”, “is there”, “what type”, “who”, and “where” are indicative of factors because they tend to have single values as responses, whereas a question such as “how to” might indicate a dimension because it, likely, requires identifying several aspects and their relations to explain the way something occurs. In some cases, wording the item as a question helps in applying this discriminant technique.

A dimension can surge when different indicators refer to the same subject. For example “cost of technology” and “technology currency” might indicate that the subject “technology” is a dimension that includes those two indicators. However, including another indicator such as “cost of training” might indicate that “cost” is also a dimension including the first and third indicator. This is because dimensions are also understood as perspectives from which to observe the subject in question, DFR in this case. Spyridopoulos & Katos (2011), for example, talk about three dimensions of cloud forensics: technical, legal and organizational.

Because there is not one single perspective that can be considered correct while excluding others, this research offers a less subjective interpretation of dimensions, and instead defines them by quantifying the recurrence of the words included in the items reclassified as dimensions. A caveat here is that in the first round of reclassification the same item may appear as both dimensions and factors or in two or more dimensions. Despite the previous explanation, distinguishing factors from dimensions is not a straightforward task. Thus, allowing items to be in different groups helps quantifying their recurrence and forces the analysis of those items in the context of other items in the extracted dimensions. The classification of dimensions is contrasted with the judgment of external reviewers via a structured methodology called Q-sort test, explained below.

4. Testing of the dimensional classification through a Q-Sort test

The content validity tests the completeness and correct classification of the words as real representations of the dimensions of DFR. This is done through a Q-Sort test. Q-Sort tests have been previously used in the literature by Davis 1989; Segars & Grover 1998; and Guo 2014, among many others.

The implementation in this study is slightly different. Those words and groups of words finally selected as potential dimensions are separated from their sets and individually presented to a group of academics and professionals of information systems for them to regroup them as they think will represent independent dimensions.

5. Adjustment of the validity of the dimensional classification using association rules

The groups selected by the exterbal reviewers are assessed in terms of the cohesion of words in a specific group and its distinction from other groups by using a data mining technique known as association rules. This is equivalent to measures of convergent and discriminant validity, as shown in the results section.

**Phase 2: Elaboration and Testing of an Instrument to Assess DFR**

6. Refinement of indicators to be used to survey organizations

Once the framework of dimensions is defined, all items are assigned to the dimension in which they better fit. In order to perform this classification two tasks are implemented. First, all 1115 items are checked via a lookup function in Excel for their containment of a word belonging to a dimension and marked accordingly. Second, all 1115 items were semantically interpreted and assigned to all dimensions where they could belong. Obviously, many items fall into several dimensions because words used to describe the item appear in several categorical dimensions or because they semantically seem to belong to several dimensions at the same time.

After separating items in dimensions, each dimension is reviewed individually to check on repeated items that could be eliminated. Once all categories are cleaned, Items are organized by unique item ID in order to detect ID duplication and decide in which of the several dimensions they will remain. Finally, those items which are semantically equivalent are merged into a single one or clustered to be redacted as measurable indicators.

The extra care and work that this stage entails is justified by the unique opportunity of conducting a structured research with qualified professionals whose available time is in shortage. Given the quantitative characteristics of this research, each qualified respondent is of paramount importance in order to assure the power of the test. Therefore, the construction of a parsimonious and optimized test is useful to avoid attrition of respondents and minimize other threats of internal validity when conducting the study.

The indicators must be tested through surveys using scales, such as the Likert scale, that allow the statistical assessment of potential predictors. Alternatively, semantic differential scales are used when considered more appropriate. The instrument also asks a pre and post survey question testing the effect of the awareness on the perceived DFR status: What is the level of forensic readiness of your organization?

After the elimination of duplicated items and grouping items based on semantic equivalence, each category comprises a reduced set of items. They are not redacted in a way that can be used in a survey. Therefore, they are reshaped into single questions that capture what they pretend to measure in terms of DFR. Some groups are summarized in a single question whereas some items need two or more questions in order to capture what they aim to assess.

7. Distinction between extant and perceptual indicators of DFR

The result is the list of measurable indicators of a survey instrument. Among them, there are questions that describe the current status of the organization. For example, if a specific training has been provided or a specific system is in place. These are called extant indicators. Demographic characteristics such as the size of the company are considered a special case of extant indicators. Other questions evaluate the opinion of the respondent regarding a condition hold by the organization. For example, whether there is management support for the DFR program. These are considered perceptual indicators.

The distinction among extant and perceptual indicators is used to contrast the real and the perceived situation of the organization regarding DFR. Extant indicators give an assessment of the level of DFR in the organization according to what has been proposed by the literature, whereas the perceptual indicators account for the perceived reflection of that reality. Those perceptual items found to be correlated with the level of DFR as measured by the extant indicators make the proposed starting point of a measurement model of DFR for social scientists.

8. Assessment of reliability and validity

A sample of randomly selected companies completes a survey with the extant and perceptual indicators. These are analized independently via exploratory factor analysis. The extant indicators are considered formative of the DFR concept; therefore, they are processed using principal components analysis. The perceptual indicators are considered reflective of the DFR concept; therefore, they are processed using maximum likelihood.

The results of the pilot study are used to assess the feasibility of these factor analyses and to have a preliminary approach of the nomological validity of the latent factors discovered in the final study. Cronbach's alpha measures are performed for the assessment of reliabilty of the indicators of the final factors.

9. Final survey and exploratory factor analysis

Statistical exploratory factor analysis is used in order to detect the latent factors behind the tested indicators. Although Churchill's general framework proposes a procedure to develop measures for marketing constructs using multi-item measures, this methodology is frequently used in other business and social disciplines. An important consideration must be done regarding the adoption of Churchill's methodology. Even though multi-item measures are utilized in the present research, Churchill's procedure is designed for reflective items and not for some of the formative items resulting here. DFR is a complex construct defined by interrelated yet independent aspects in the organization. For this reason, some of the factors of interest of this study are mostly formative rather than reflective factors. Therefore, the evaluations of reliability through tests such as Cronbach's Alpha have limitations in assessing the items of the final scale. Formative indicators may not respond as expected to the reliability tests even though they indeed belong to the factor of interest. This issue requires the following short clarification.

**Formative vs. Reflective Factors**

Formative factors are conceived as the pillars of a composite variable hence this variable owes its existence to the presence of each of those factors in an additive way. In other words, we understand that the composite variable exists because the factors exist simultaneously. On the other hand, reflective factors are indications that a latent variable is present. Therefore, when the latent variable changes all their indicators change to reflect that change. In the case of formative factors, not all indicators need to change in order to see a change in the latent variable, i.e., they are not expected to correlate. Because the causal flow is different from formative to reflective factors, the indicators are exchangeable in the reflective case and definitional in the formative case (Rash.org 2015 retrieved on 150622 from http://www.rasch.org/rmt/rmt221d.htm).

The definition of indicators as formative or reflective must then be justified by the researcher based on sound theory more than statistics. Notwithstanding, statistical analysis can open the door to reevaluate the theory. As an example, let us use Elyas et al. (2014) summary of DFR in three goals and turn them into measurable indicators:

1. My organization is ready to collect and present valid digital evidence in the event of digital crime.
2. My organization is ready to collect and present valid digital evidence in the event of litigation.
3. My organization is ready to collect and present valid digital evidence in the event of internal dispute.

An assessment of DFR under this perspective seems to be formative because the organization's status on DFR depends on the combined status of three different indicators. They are: readiness to provide evidence in a digital crime, readiness to do it in case of litigation, and readiness to do it in case of internal dispute. However, a high correlation among the items associated to all of them might indicate that these factors are indeed reflective rather than formative. This is, perhaps, because although DFR is achieved through several independent ways, once a certain level of DFR is gained it will simultaneously improve the ability to collect and present digital evidence regardless of the reason why this collection is done.

This said, measures of reliability are implemented in this research regardless of the classification of indicators. According to Davis (1989) who uses this methodology in the development of the technology acceptance model (TAM), the appropriate selection of the initial scale items helps to assure the content validity of the scales. Far from avoiding the theoretical discussion on the issues explained above, this study aims to encourage it.

## 10. Conclusions, assumptions, limitations and contributions of the study

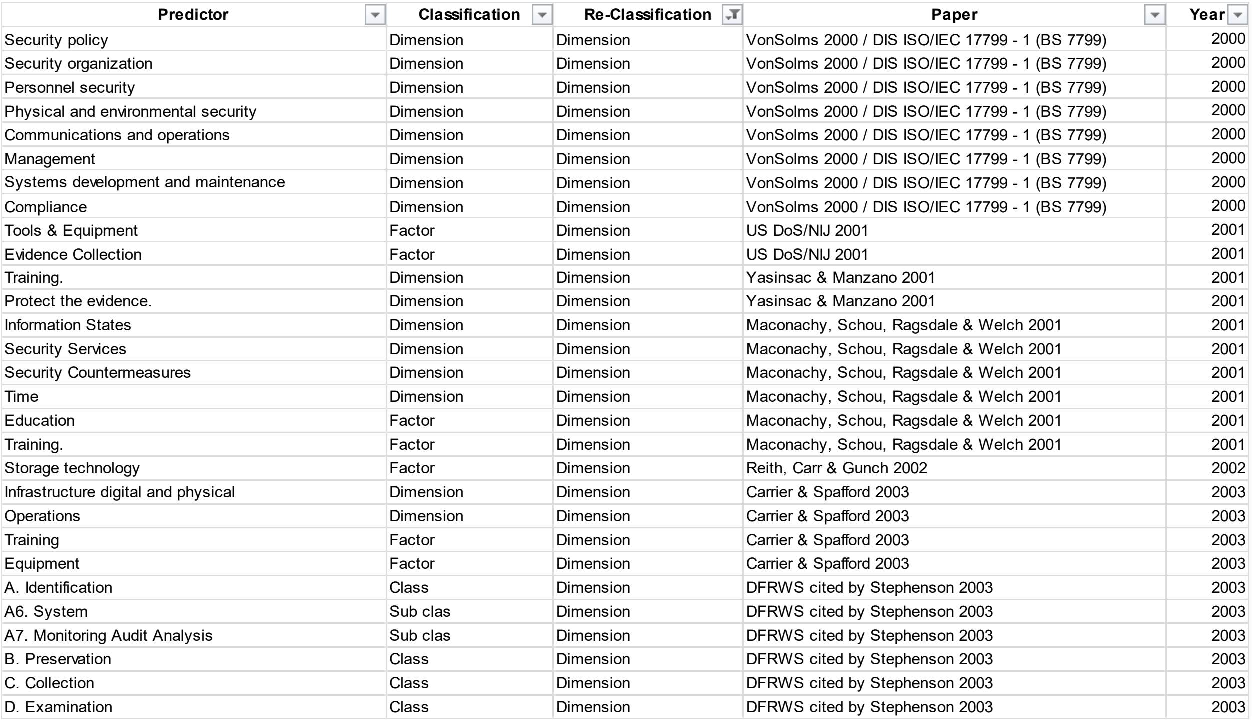
This process is as real a measure of DFR as it can be, considering the unattainable conditions of a definitive assessment. Yet, the proposed tasks have their own challenges as well. Some assumptions and limitations hold and are explained after the concluding remarks of the study.

This methodology not only values the theoretical and practical knowledge on DFR, but also combines qualitative and quantitative techniques whenever they are more convenient in order to guarantee that the research follows a structured process that is testable and repeatable. In particular, this study uses Q-Sort tests as a structured way to extract information from experts and statistical techniques on all quantifiable data.

# CHAPTER IV

## RESULTS

1115 potential indicators of DFR where extracted from the literature. This list is found as Appendix A. Of those 1115 potential indicators of DFR, 381 items were considered to be representative of dimensions. A snapshot showing a partial section of a table of items reclassified as dimensions is in Figure 4. The complete table of 381 items is too large to be included in the body of this paper; hence, it is provided as Appendix B.



| Predictor | Classification | Re-Classification | Paper | Year |
|---|---|---|---|---|
| Security policy | Dimension | Dimension | VonSolms 2000 / DIS ISO/IEC 17799 - 1 (BS 7799) | 2000 |
| Security organization | Dimension | Dimension | VonSolms 2000 / DIS ISO/IEC 17799 - 1 (BS 7799) | 2000 |
| Personnel security | Dimension | Dimension | VonSolms 2000 / DIS ISO/IEC 17799 - 1 (BS 7799) | 2000 |
| Physical and environmental security | Dimension | Dimension | VonSolms 2000 / DIS ISO/IEC 17799 - 1 (BS 7799) | 2000 |
| Communications and operations | Dimension | Dimension | VonSolms 2000 / DIS ISO/IEC 17799 - 1 (BS 7799) | 2000 |
| Management | Dimension | Dimension | VonSolms 2000 / DIS ISO/IEC 17799 - 1 (BS 7799) | 2000 |
| Systems development and maintenance | Dimension | Dimension | VonSolms 2000 / DIS ISO/IEC 17799 - 1 (BS 7799) | 2000 |
| Compliance | Dimension | Dimension | VonSolms 2000 / DIS ISO/IEC 17799 - 1 (BS 7799) | 2000 |
| Tools & Equipment | Factor | Dimension | US DoS/NIJ 2001 | 2001 |
| Evidence Collection | Factor | Dimension | US DoS/NIJ 2001 | 2001 |
| Training. | Dimension | Dimension | Yasinsac & Manzano 2001 | 2001 |
| Protect the evidence. | Dimension | Dimension | Yasinsac & Manzano 2001 | 2001 |
| Information States | Dimension | Dimension | Maconachy, Schou, Ragsdale & Welch 2001 | 2001 |
| Security Services | Dimension | Dimension | Maconachy, Schou, Ragsdale & Welch 2001 | 2001 |
| Security Countermeasures | Dimension | Dimension | Maconachy, Schou, Ragsdale & Welch 2001 | 2001 |
| Time | Dimension | Dimension | Maconachy, Schou, Ragsdale & Welch 2001 | 2001 |
| Education | Factor | Dimension | Maconachy, Schou, Ragsdale & Welch 2001 | 2001 |
| Training. | Factor | Dimension | Maconachy, Schou, Ragsdale & Welch 2001 | 2001 |
| Storage technology | Factor | Dimension | Reith, Carr & Gunch 2002 | 2002 |
| Infrastructure digital and physical | Dimension | Dimension | Carrier & Spafford 2003 | 2003 |
| Operations | Dimension | Dimension | Carrier & Spafford 2003 | 2003 |
| Training | Factor | Dimension | Carrier & Spafford 2003 | 2003 |
| Equipment | Factor | Dimension | Carrier & Spafford 2003 | 2003 |
| A. Identification | Class | Dimension | DFRWS cited by Stephenson 2003 | 2003 |
| A6. System | Sub clas | Dimension | DFRWS cited by Stephenson 2003 | 2003 |
| A7. Monitoring Audit Analysis | Sub clas | Dimension | DFRWS cited by Stephenson 2003 | 2003 |
| B. Preservation | Class | Dimension | DFRWS cited by Stephenson 2003 | 2003 |
| C. Collection | Class | Dimension | DFRWS cited by Stephenson 2003 | 2003 |
| D. Examination | Class | Dimension | DFRWS cited by Stephenson 2003 | 2003 |

Figure 4. Items re-classified as potential dimensions of DFR (Partial View)

The number of items discovered is too big, which makes it difficult to make sense of the potential dimensions by identifying groups of similar indicators that are at the same time different to indicators in other groups. Thus, a semantic approach is used to discover the underlying dimensions to which these items belong. It consists of finding the recurrent terms used by authors when describing indicators, grouping those words that are semantically equivalent, and counting their recurrence throughout the set of items. The process so far explained can be summarized as follows:

1. Identify each item as a factor or dimension
2. Extract those items classified as dimensions
3. Select recurrent words that appear within the selected items indicative of dimensions
4. Group those words which are semantically equivalent
5. Create a matrix of word sets (in columns) versus items (in rows)
6. Compare each item against each word set and give it a point if the item contains the word or a synonym of it
7. Add the total points for each word to show its weight according to the recurrence in the list (higher counts are considered more indicative of a dimension)

The list of 128 word sets initially selected as potential dimensions of DFR comprises: Accelerate, Access, Accreditation/Compliance/Certify, Action/Activity, Admissible/Credible, Advise, Alert, Analysis/Intelligence, Anonymous, Apply/Conduct/Establish/Execute/Implement/Perform, Approve, Architecture, Archive/Custody/Preserve/Protect/Storage, Assessment/Measure/Indicator/Statistics/Test, Asset, Assurance, Attack/Risk/Threat, Audit, Authenticate/Authorize/Identity/Log (people), Available, Awareness, Best Practice, Business, Capability/Ability, Case/Event/Incident, Chain/Flow, Cloud, Code/Guideline/Law/Requirement/Rule, Collaborate/Interact, Collect/Acquire/Extract/Retain, Commitment, Communicate/Disseminate/Notify/Present/Report, Computer/Hardware/Server, Contact, Containment/Defense/Resilience, Context/Environment/External, Control, Coordinate, Cost, Create, Culture, Customer, Data/Information/Record, Delete, Demonstration/Evidence/Proof, Detection/Monitoring/Surveillance, Deter/Disrupt/Interrupt/Limit, Develop, Digital, Document, Education/Training, Electronic, Emergency, Enforcement, Escalate, Forensic, Formal, Functionality, Governance, Hierarchy/Structure, Hypothesis, Identify/Classify, Impact, Industry, Infrastructure, Integrity, Inter/Multi-disciplinary, Internal, Intrusion, Investigate, Expertise/Knowledge/Literacy/Skill, Lab, Lead, Live, Maintenance, Manage/Adm/Handling, Mature, Media, Mitigate/Minimize, Mobile, Model, Need, Network, Objective, Obligation, Organization/Corporate, People/Personnel/Stakeholder/User, Physical, Plan, Policy, Prepare/Prevent, Privilege, Procedure/Process/Operation/Method, Professional, Program, Prosecute, Quality/Effectiveness, Readiness, Recover, Reliable, Reputation/Status, Resource, Response, Responsibility/Role, Review, Search, Security, Select, Service, Social, Software, Source, Space/Location, Standard, Strategy, Support, System, Target, Task, Team, Technique/Technology, Time, Tools/Equipment, Traceability, Transport, Use, Wireless.

The repetition of nominations indicates consensus, throughout the literature, on the existence of a relevant dimension denoted by the word(s), while allowing reduction of the number of potential dimensions. Indicator items that do not contain any of the words of the selected dimensions, are then assigned to a created dimension, grouped together to make other eventual dimensions, left alone as an independent dimension or reconsidered as a factor.

It became clear, from this selection, that indicators of DFR classified under this framework of dimensions would belong to many of them at the same time. In addition, 128 dimensions are too many to be useful for a practical framework. Further analysis revealed that each one of the 128 terms belongs to one of three categories of words, those which refer to entities, those referring to actions, and those referring to conditions. The impact list of Table 1 below shows the number of items associated to each word from the most to the least frequent, and their classification into these three types of words.

Table 1. Frequency impact of word sets indicating dimensions

| Terms Impact List | | | |
|---|---|---|---|
| **Index** | **Term** | **Count** | **Type** |
| 1 | Procedure/Process/Operation/Method | 56 | Entity |
| 2 | Archive/Custody/Preserve/Protect/Storage | 47 | Action |
| 3 | Demonstration/Evidence/Proof | 47 | Entity |
| 4 | Data/Information/Record | 46 | Entity |
| 5 | Code/Guideline/Law/Requirement/Rule | 45 | Entity |
| 6 | Forensic | 42 | Condition |
| 7 | Security | 39 | Condition |
| 8 | Policy | 37 | Entity |
| 9 | Digital | 33 | Condition |
| 10 | People/Personnel/Stakeholder/User | 31 | Entity |
| 11 | Technique/Technology | 30 | Entity |
| 12 | Manage/Adm/Handling | 27 | Action |
| 13 | Case/Event/Incident | 26 | Entity |
| 14 | Collect/Acquire/Extract/Retain | 23 | Action |
| 15 | Education/Training | 20 | Condition |
| 16 | Expertise/Knowledge/Literacy/Skill | 20 | Condition |
| 17 | Investigate | 20 | Action |
| 18 | Analysis/Intelligence | 19 | Action |
| 19 | Organization/Corporate | 17 | Entity |
| 20 | Response | 17 | Action |
| 21 | System | 17 | Entity |
| 22 | Accreditation/Compliance/Certify | 16 | Condition |
| 23 | Computer/Hardware/Server | 15 | Entity |
| 24 | Tools/Equipment | 15 | Entity |
| 25 | Plan | 14 | Entity |
| 26 | Chain/Flow | 13 | Entity |
| 27 | Deter/Disrupt/Interrupt/Limit | 13 | Action |
| 28 | Communicate/Disseminate/Notify/Present/Report | 12 | Action |
| 29 | Detection/Monitoring/Surveillance | 12 | Condition |
| 30 | Attack/Risk/Threat | 11 | Entity |
| 31 | Capability/Ability | 11 | Condition |
| 32 | Develop | 11 | Action |
| 33 | Premises/Site/Space/Workspace | 10 | Entity |
| 34 | Apply/Conduct/Establish/Execute/Implement/Perform | 9 | Action |
| 35 | Authenticate/Authorize/Identity/Log (people) | 9 | Action |
| 36 | Awareness | 9 | Condition |
| 37 | Business | 9 | Entity |
| 38 | Context/Environment/External | 9 | Entity |
| 39 | Infrastructure | 9 | Entity |
| 40 | Maintenance | 9 | Condition |
| 41 | Prepare/Prevent | 9 | Action |
| 42 | Team | 9 | Entity |
| 43 | Document | 8 | Entity |
| 44 | Network | 8 | Entity |
| 45 | Responsibility/Role | 7 | Condition |
| 46 | Admissible/Credible | 6 | Condition |
| 47 | Architecture | 6 | Entity |

|  |  |  |  |
|---|---|---|---|
| 48 | Assessment/Measure/Indicator/Statistics/Test | 6 | Action |
| 49 | Cloud | 6 | Entity |
| 50 | Governance | 6 | Condition |
| 51 | Identify/Classify | 6 | Action |
| 52 | Integrity | 6 | Condition |
| 53 | Readiness | 6 | Condition |
| 54 | Anonymous | 5 | Condition |
| 55 | Collaborate/Interact | 5 | Action |
| 56 | Control | 5 | Action |
| 57 | Cost | 5 | Condition |
| 58 | Culture | 5 | Condition |
| 59 | Enforcement | 5 | Condition |
| 60 | Jurisdiction | 5 | Condition |
| 61 | Physical | 5 | Condition |
| 62 | Resource | 5 | Entity |
| 63 | Software | 5 | Entity |
| 64 | Accelerate | 4 | Action |
| 65 | Action/Activity | 4 | Action |
| 66 | Hierarchy/Structure | 4 | Condition |
| 67 | Inter/Multi-disciplinary | 4 | Condition |
| 68 | Internal | 4 | Condition |
| 69 | Program | 4 | Entity |
| 70 | Quality/Effectiveness | 4 | Condition |
| 71 | Transport | 4 | Action |
| 72 | Use | 4 | Condition |
| 73 | Approve | 3 | Action |
| 74 | Assurance | 3 | Condition |
| 75 | Audit | 3 | Action |
| 76 | Available | 3 | Condition |
| 77 | Containment/Defense/Resilience | 3 | Condition |
| 78 | Coordinate | 3 | Action |
| 79 | Hypothesis | 3 | Entity |
| 80 | Lead | 3 | Action |
| 81 | Strategy | 3 | Entity |
| 82 | Asset | 2 | Entity |
| 83 | Commitment | 2 | Condition |
| 84 | Electronic | 2 | Condition |
| 85 | Formal | 2 | Condition |
| 86 | Intrusion | 2 | Entity |
| 87 | Lab | 2 | Entity |
| 88 | Live | 2 | Condition |
| 89 | Mitigate/Minimize | 2 | Action |
| 90 | Reliable | 2 | Condition |
| 91 | Review | 2 | Action |
| 92 | Standard | 2 | Condition |
| 93 | Time | 2 | Entity |
| 94 | Traceability | 2 | Condition |
| 95 | Access | 1 | Condition |
| 96 | Advise | 1 | Action |
| 97 | Alert | 1 | Action |

| | | | |
|---|---|---|---|
| 98 | Best Practice | 1 | Condition |
| 99 | Contact | 1 | Action |
| 100 | Create | 1 | Action |
| 101 | Customer | 1 | Entity |
| 102 | Delete | 1 | Action |
| 103 | Emergency | 1 | Condition |
| 104 | Escalate | 1 | Action |
| 105 | Functionality | 1 | Condition |
| 106 | Impact | 1 | Condition |
| 107 | Industry | 1 | Condition |
| 108 | Mature | 1 | Condition |
| 109 | Media | 1 | Entity |
| 110 | Mobile | 1 | Condition |
| 111 | Model | 1 | Condition |
| 112 | Need | 1 | Condition |
| 113 | Objective | 1 | Entity |
| 114 | Obligation | 1 | Condition |
| 115 | Privilege | 1 | Condition |
| 116 | Professional | 1 | Condition |
| 117 | Prosecute | 1 | Action |
| 118 | Recover | 1 | Action |
| 119 | State | 1 | Condition |
| 120 | Search | 1 | Action |
| 121 | Select | 1 | Action |
| 122 | Service | 1 | Action |
| 123 | Social | 1 | Condition |
| 124 | Source | 1 | Entity |
| 125 | Support | 1 | Condition |
| 126 | Target | 1 | Entity |
| 127 | Task | 1 | Entity |
| 128 | Wireless | 1 | Condition |

These categories can be dimensions by themselves because they present different perspectives from which to approach the problem. This means that the DFR status can be seen from the perspective of the processes involved, from the perspective of certain conditions that together represent the DFR status or from the perspective of which entities, on which those conditions and processes operate, must be considered to evaluate the level of DFR in an organization. In addition, the interactions among the three groups of words, naturally describe indicators of DFR status. Entities can be the object and subject of different processes and achieve different conditions. Processes can also fulfill or achieve a specific condition.

One reason to not use these three categories of words as dimensions is that each would include too many indicators as many other terms within each category seem to be relevant and independent from the others. Another reason is their poor usefulness in helping to discriminate indicators. Let us take an example. Imagine that we classify students into those who study biology, those who are above 21 years old, and those who are born in California. Several students would belong to all categories at the same time. Therefore, the dimensions major, age and birth place would lack discriminant validity. Therefore, we should choose either major, age or birthplace as a first level of categorization. Likewise, we should choose either entities, conditions or actions as a first level of categorization because indicators can easily belong to all of the simultaneously. Despite the reasonableness of this approach it is hardly adopted in the reviewed literature. For the purpose of this research, minimizing overlapping among dimensions is important.

Although any of the groups of word sets can be selected as the initial perspective, conditions and actions are slightly more conceptual whereas entities include mostly tangible elements or elements of easier recognition. A glimpse to the impact list of this word sets in Table 1, also reveals the prevalence of entities at the top of the list - half of the top 30 words are entities -, which indicates that more indicators can be directly classified according to the entity they refer to than according to an action or condition they refer to. Therefore, only word groups representing entities will be used as potential dimensions. Because all actions and conditions found owe their existence to their association to one of the entities, any relevant factor of DFR will be classified into at least one dimension. Moreover, all actions are included in the "Procedure/Process/Operation/Method" entity because all actions are themselves a process or a stage in a process. The "Entities" group comprises terms such as procedures, data, people, and law, which are expected to define the domains within which indcators are circumscribed. By implementing this methodology the space of possible dimensions is reduced to 42. The following list shows the set of words grouped as entities with their respective impact.

Table 2. Word sets indicating dimensions classified as entities

| Term | Count |
|---|---|
| Procedure/Process/Operation/Method | 56 |
| Demonstration/Evidence/Proof | 47 |
| Data/Information/Record | 46 |
| Code/Guideline/Law/Requirement/Rule | 45 |
| Policy | 37 |
| People/Personnel/Stakeholder/User | 31 |
| Technical/Technology | 30 |
| Case/Event/Incident | 26 |
| Organization/Corporate | 17 |
| System | 17 |
| Computer/Hardware/Server | 15 |
| Tools/Equipment | 15 |
| Plan | 14 |
| Chain/Flow | 13 |
| Attack/Risk/Threat | 11 |
| Premises/Site/Space/Workspace | 10 |
| Business | 9 |
| Context/Environment/External | 9 |
| Infrastructure | 9 |
| Team | 9 |
| Document | 8 |
| Network | 8 |
| Architecture | 6 |
| Cloud | 6 |
| Resource | 5 |
| Software | 5 |
| Program | 4 |
| Hypothesis | 3 |
| Strategy | 3 |
| Asset | 2 |
| Intrusion | 2 |
| Lab | 2 |
| Time | 2 |
| Customer | 1 |
| Media | 1 |
| Objective | 1 |
| Service | 1 |
| Source | 1 |
| Target | 1 |
| Task | 1 |

Several terms show high recurrence among the items extracted from the literature, while other terms with fewer repetitions seem to be relevant and independent enough to be included as unique dimensions. There is, however, a big difference between the top and the bottom of the list in terms of recurrence. While terms at the top repeat tens of times, there are several terms at the bottom that appear only one or few times throughout the items selected as dimensions. Although the lack of convergence around a term among authors may indicate that such terms are not dimensions, it can also mean that some of these terms can be regrouped into better defined dimensions.

For example, the terms Plan, Program, Objective, Target, Task and Strategy are all elements of the digital forensics strategic plan of the organization and can be put together; the term Document fits well with Data, Information goes with Record; Intrusion can be grouped with Attack, Risk and Threat go well together; Business goes with Organization/Corporate; Customer and Team can join the terms referring to People; Assets fits with Resources; Lab with Workspace; and Tools/Equipment with Computer and Hardware. In the context of the new list, the term Policy, which makes a category by itself with 37 counts, could be placed at the same level of Rules and Guidelines, which as a group are distinct from all other terms. These associations among terms would have been very difficult to detect in earlier stages of this research.

As for the low-frequency terms that remain in the list (i.e. Hypothesis, Time, Media and Source), a second look at their originator items gives important information to make decisions on them as potential dimensions or not. The three times that the term Hypothesis shows up, it originates from the same paper, hence there is probably not a real recurrence in the literature for it, and it can be discarded as a dimension. The term Time comes from two different papers, and it is the judgement of the researchers that Time gives a relevant and unique perspective as to be kept as a potential dimension. Source and Media appear a single time each and might not be good descriptors of dimensions. The regrouping of word sets of potential dimensions with their aggregate counts is listed below.

Table 3. Potential dimensions extracted from Literature Review

| Dimensions | Count |
|---|---|
| Code/Guideline/Law/Policy/Requirement/Rule | 82 |
| Procedure/Process/Operation/Method | 56 |
| Data/Document/Information/Record | 54 |
| Demonstration/Evidence/Proof | 47 |
| Customer/People/Personnel/Stakeholder/Team/User | 41 |
| Computer/Equipment/Hardware/Server/Tools | 30 |
| Technical/Technology | 30 |
| Case/Event/Incident | 26 |
| Business/Corporate/Organization | 26 |
| Plan/Program/Strategy/Objective/Target/Task | 24 |
| System | 17 |
| Chain/Flow | 13 |
| Attack/Intrusion/Risk/Threat | 13 |
| Lab/Premises/Site/Space/Workspace | 12 |
| Context/Environment/External | 9 |
| Infrastructure | 9 |
| Network | 8 |
| Asset/Resource | 7 |
| Architecture | 6 |
| Cloud | 6 |
| Software | 5 |
| Time | 2 |

It seems like these 22 groups of words selected represent the most internally consistent and externally differentiated categories where DFR factors can be placed. However, this selection is submitted to the judgement of qualified reviewers in order to validate the discriminant and convergent validity of the groups through a Q-Sort test.

**Q-Sort Test**

The 22 selected dimensions include 65 words. The reviewers are given the 65 words, which they classify in as few as possible unique categories containing only the words required to give sense to the dimension. This is a slight variation over conventional Q-sort tests in that no pre-established categories were suggested to respondents. Reviewers were free to assign as many categories as they wanted, each with as many words as they deemed appropriate.19 reviewers completed the Q-sort test. They are either technical people with experience in information systems and security, graduate students in information systems or computer sciences, or faculty. Each reviewer worked independently. All tests took place in

December, 2015. The instructions for the classification task can be seen in Appendix C. A summary of the demographics of respondents is shown below as number of respondents in each category:

Table 4. Respondents' demographics from Q-Sort Test (Age)

| **Reviewer's Age** | |
|---|---|
| Below 18 (1) | 0 |
| 18 to 25 (2) | 2 |
| 26 to 33 (3) | 6 |
| 34 to 41 (4) | 4 |
| 42 to 49 (5) | 4 |
| 50 to 57 (6) | 2 |
| Above 57 (7) | 1 |

Table 5. Respondents' demographics from Q-Sort Test (Gender)

| **Reviewer's Gender** | |
|---|---|
| Male (1) | 11 |
| Female (2) | 8 |

Table 6. Respondents' demographics from Q-Sort Test (IS Experience)

| **Reviewer's Experience in Information Systems** | |
|---|---|
| Less than 1 (1) | 0 |
| 1 to 5 (2) | 3 |
| 6 to 10 (3) | 4 |
| 11 to 15 (4) | 3 |
| 16 to 20 (5) | 5 |
| 21 to 25 (6) | 0 |
| More than 25 (7) | 4 |

Table 7. Respondents' demographics from Q-Sort Test (InfoSec Experience)

| **Reviewer's Experience in Information Security** | |
|---|---|
| Less than 1 (1) | 4 |
| 1 to 5 (2) | 6 |
| 6 to 10 (3) | 4 |
| 11 to 15 (4) | 2 |
| 16 to 20 (5) | 1 |
| 21 to 25 (6) | 1 |
| More than 25 (7) | 1 |

Table 8. Respondents' demographics from Q-Sort Test (Self-Assessment)

| Reviewer's Selfvaluation of Expertise in Security | |
|---|---|
| Layman (1) | 2 |
| Minimal (2) | 1 |
| Below average (3) | 0 |
| Average (4) | 2 |
| Above average (5) | 7 |
| Superior (6) | 5 |
| Expert (7) | 2 |

The results of the sorting were organized and prepared for analysis using Microsoft Excel. The file with the raw data was named Data0 and imported into R (the open source and domain-specific programming language for statistics and data analysis). This research applies an unsupervised data mining technique called association rules in order to detect possible dimensions. Association rules are the algorithms used to perform market basket analysis through which the co-occurrence of products among transactions in a store is looked for in order to gain insights on cross-selling opportunities. It was deemed appropriate to apply the same technique in this research because the occurrence of products in transactions is very similar to the occurrence of words in selected categories chosen by respondents of the Q-sort test.

Two differences exist between these two scenarios. First, whereas basket analysis aims to find causation relationships between products, the sole coexistence of words is enough indication of a category in this research. Second, unlike transactions, where a product can be not purchased at all or appear many more times than others, in our categories each word appears exactly as many times as respondents completing the classification task. These characteristics are important in defining the minimum value of parameters to assess the validity of the dimensions.

One of the earliest and most fundamental algorithms for generating association rules is called Apriori (EMC 2015 Data Science and Big data analytics). The application of the apriori algorithm requires the creation of a model under which rules of association are created by R. Although the rules of association are found by the software in an unsupervised way, the parameters of the model must be defined by the researcher. In particular, values for the support, confidence and minimum length parameters must be entered.

The minimum length refers to the minimum number of items that are expected in a group or an itemset. Itemset is the generic term used by data miners using association rules for what this research calls groups of words or group sets, categories or potential dimensions. For our case, the minimum number for an itemset is two (2) because the research is trying to find which of the 65 words can be put together in a category in order to reduce the potential number of categories, and at least one pair of words will suffice to make a category.

The support parameter refers to the proportion of a specific itemset (a word or group of words) that is expected to be found among the selections of respondents. In this research, there are 19 respondents; hence, itemsets that are selected by at least 10 respondents have the support of the majority. Given that the total itemsets selected by the 19 respondents is 252 (see summary of Data0 below), the minimum value for the support parameter is 10/252 or 0.03968254. Beacuse an itemset cannot be selected more than once by a respondent, the maximum possible support for any itemset is 19/252 or 0.075396825.

The confidence value indicates the probability that an itemset A is chosen in a selection given that another itemset B was chosen in the same selection. This probability is calculated by comparing the total times that the itemset A is selected with the total times that the itemset A is selected along with the given itemset B. In our case, each given itemset (a word or group of words) is selected exactly 19 times, once by each respondent. Therefore, an acceptable value for confidence that an itemset A implies the presence of another itemset B in the same selection is that at least 10 respondents put itemset A and itemset B together in the same category. This value is 10/19 or 0.5263.

### Analysis of Q-Sort Test Using Data Mining Association Rules

Once the data is collected from the Q-sort tests, it is organized and imported to R, where the summary(data) instruction provides the characteristics of the data set:

```
Summary of Data0
Categories as itemMatrix in sparse format with:
252 rows (Itemsets/categories)
65 columns (items) and a density of 0.07539683
Most frequent items:
```

```
Architecture     Asset            Attack           Business                  Case    (Other)
19               19               19               19               19       1140
Itemset/Category length distribution:
Sizes: 1  2  3  4  5  6  7  8  9 10 11 12 13 16 17 18 21 22
Number of categories: 43 28 35 30 25 28 23  7  6  8  6  2  5  1  1  2  1  1
Descriptive Statistics:
Min.     1st Qu.   Median  Mean    3rd Qu.    Max.
1.000    2.000     4.000    4.901   6.250      22.000
```

In the R output shown above, 252 rows indicate that a total of 252 categories were selected; “65 columns” indicate the number of words to be classified. The “Most frequent items” is a list of the top five words most chosen (which in our case is irrelevant because all words are chosen 19 times, although it confirms that all selections are complete). The “Itemset/Category length distribution” shows the frequency of categories’ sizes. For example, categories of one element where chosen 43 times, while categories of 17, 18, 21 and 22 words were chosen only once each. Finally, the “Descriptive statistics” show that the minimum words per category is one, while the maximum is 22, and the average size of a category in number of words is close to 5.

Our sparse matrix has a size of 16,380 (252 groups times 65 words) and a density of 0.07539683. This indicates that 1,235 selections were made (16380*0.07539683), which is correct because each of the 19 respondents assigned each of the 65 words (19*65=1,235). This is another way to assure that no words were missing or misspelled or counted twice. Excel’s filters and find functions were also used to assure this. The 19 respondents chose a total of 252 groups or categories, which gives an average of 13.26 dimensions per respondent (252/19). The mean size of a group is 4.9, but it must be an integer number, so we should say it is 5. Data0 is used as the raw data to create the model called Model0 with the parameters adopted. The instruction to build Model0 in R is: `> Model0<-apriori(Data0, parameter = list(support=0.03968, confidence=0.5263, minlen=2)).`

The first part of the output (attached in Appendix D to facilitate replication of the analysis), show the type of algorithm implemented (Apriori), the values of the parameters used by the algorithm, and times of internal operations in the computations.

The summary of Model0 below shows that, under these conditions, the algorithm finds 403 rules of which 156 involved 2 words, 135 rules involved 3 words, 76 rules involved 4 words, 30 rules involved 5 words, and 6 rules involved 6 words. The “lhs” and “rhs” terms in the output refer to the left and right hand sides of the rules, respectively. This is because, as explained above, the Apriori algorithm is mostly used for market basket analysis looking for rules where the existence of a product on the left implies the purchase of a product on the right. In our case, only the coexistence of words (instead of products) in a category (instead of a transaction) is relevant.

```
Summary of Model0
Set of 403 rules
Rule length distribution (lhs + rhs): sizes
2       3       4       5       6
156     135     76      30      6
Min.    1st Qu. Median  Mean    3rd Qu. Max.
2.000   2.000   3.000   2.995   4.000   6.000
Summary of quality measures:
   Support              confidence              lift
Min.:   0.03968         Min.:   0.5263          Min.:   6.981
1st Qu.:0.04365         1st Qu.:0.6842          1st Qu.:        9.075
Median:0.04762          Median:0.8421           Median:11.169
Mean:   0.04922         Mean:   0.8176          Mean:   10.844
3rd Qu.:        0.05357         3rd Qu.:        0.9474          3rd Qu.:                12.565
Max.:   0.07540         Max.:   1.0000          Max.:   13.263
Mining info:
Data; Data0
Ntransactions: 252
Support: 0.03968
Confidence: 0.5263
```

The complete set of rules is available as Appendix D, and can be obtained with the instruction > inspect(Model0) in R. 403 rules result from the application of the model using the selected parameters. The rules suggest that some words are associated with others in what can be considered a dimension of DFR. However, many of the rules are redundant for the purpose of this research. This happens for two reasons: first, unlike common transactions where products can be selected never or many times in a group of transactions, words in this research are selected once by each respondent and thus appear the same number of times (N) in the group of selections. If two words A and B appear together only once, they both will appear N-1 times not together; hence, both have the same confidence. If the association of these words passes the minimum parameter test of Model0, two rules will show up, one with word A implying word B and another with word B implying word A. Association of more words follow similar logic.

The second reason for redundancy is that rules associating a subset of words that are contained within bigger sets of associated words in other accepted rules are unnecessary. For example, if a suggestion is accepted from a rule associating words A, B and C, six other accepted rules are redundant:

A implying B, B implying A, B implying C, C implying B, A implying C, and C implying A. Thus, only the rule involving A, B and C should be kept.

After trimming off unnecessary rules, only 36 rules remain. They are shown in Table 5 in the original format resulting from R, and with their respective original number as posted in Appendix D, in order to facilitate tracking down the trimming process. The rules are grouped in clusters representing the dimensions found after the Q-sort test. Some of them, such as rules 335, 216, and 403, are exact representations of researcher's choice of dimensions, which is meaningful given that reviewers were completely free to associate words in dimensions. Rule 363 involving four words was also predicted by the researcher, except for a fifth word not included by the reviewers.

Table 9. Potential dimensions after application of association rules algorithm

| # | Rule | | | Support | Confidence | Lift |
|---|---|---|---|---|---|---|
| 335 | {Attack,Intrusion,Risk} | => | {Threat} | 0.048 | 1.000 | 13.263 |
| 359 | {Attack,Event,Incident} | => | {Intrusion} | 0.040 | 1.000 | 13.263 |
| 252 | {Attack,Target} | => | {Intrusion} | 0.040 | 1.000 | 13.263 |
| 17 | {Threat} | => | {Target} | 0.040 | 0.526 | 6.981 |
| 234 | {Site,Space} | => | {Workspace} | 0.040 | 1.000 | 13.263 |
| 235 | {Site,Workspace} | => | {Premises} | 0.040 | 0.833 | 11.053 |
| 240 | {Premises,Space} | => | {Workspace} | 0.040 | 1.000 | 13.263 |
| 243 | {Environment,Space} | => | {Workspace} | 0.040 | 0.833 | 11.053 |
| 54 | {Premises} | => | {Workspace} | 0.048 | 0.632 | 8.377 |
| 57 | {Workspace} | => | {Lab} | 0.040 | 0.526 | 6.981 |
| 63 | {Site} | => | {Environment} | 0.040 | 0.526 | 6.981 |
| 93 | {Proof} | => | {Case} | 0.040 | 0.526 | 6.981 |
| 91 | {Evidence} | => | {Proof} | 0.063 | 0.842 | 11.169 |
| 85 | {Record} | => | {Document} | 0.040 | 0.526 | 6.981 |
| 95 | {Information} | => | {Data} | 0.063 | 0.842 | 11.169 |
| 279 | {Guideline,Strategy} | => | {Plan} | 0.040 | 1.000 | 13.263 |
| 120 | {Strategy} | => | {Objective} | 0.040 | 0.526 | 6.981 |
| 100 | {Policy} | => | {Requirement} | 0.040 | 0.526 | 6.981 |
| 87 | {Law} | => | {Rule} | 0.048 | 0.632 | 8.377 |
| 131 | {Policy} | => | {Procedure} | 0.040 | 0.526 | 6.981 |
| 275 | {Guideline,Rule} | => | {Policy} | 0.040 | 0.909 | 12.057 |
| 147 | {Guideline} | => | {Procedure} | 0.044 | 0.579 | 7.679 |
| 155 | {Method} | => | {Procedure} | 0.040 | 0.526 | 6.981 |
| 135 | {Process} | => | {Procedure} | 0.048 | 0.632 | 8.377 |
| 133 | {Process} | => | {Flow} | 0.040 | 0.526 | 6.981 |
| 102 | {Process} | => | {Operation} | 0.056 | 0.737 | 9.773 |
| 89 | {Resource} | => | {Asset} | 0.052 | 0.684 | 9.075 |
| 216 | {Corporate,Organization} | => | {Business} | 0.052 | 1.000 | 13.263 |
| 127 | {Architecture} | => | {Infrastructure} | 0.044 | 0.579 | 7.679 |
| 273 | {Code,Software} | => | {Program} | 0.044 | 0.846 | 11.223 |
| 97 | {System} | => | {Software} | 0.040 | 0.526 | 6.981 |
| 363 | {Computer,Hardware,Server} | => | {Equipment} | 0.052 | 0.867 | 11.495 |
| 367 | {Computer,Hardware,Network} | => | {Server} | 0.040 | 0.909 | 12.057 |
| 265 | {Equipment,Network} | => | {Hardware} | 0.040 | 1.000 | 13.263 |
| 137 | {Technology} | => | {Computer} | 0.040 | 0.526 | 6.981 |
| 403 | {Customer,People,Personnel,Team,User} | => | {Stakeholder} | 0.044 | 0.917 | 12.158 |

### Adjustment of Framework Based on Results of Q-sort Test

Exact coincidences, however, were not expected. Instead, patterns of words that frequently appear together in reviewers' selections are looked for. These co-occurrences are even more meaningful if those words in identified dimensions do not appear in distinct dimensions, thus reinforcing the characteristics of internal validity within the groups and external validity among them.

The 36 rules summarizing all supported co-occurrences display 12 distinct dimensions with no overlapping among them. These rules include 56 out of the 65 words presented. If each of the nine remaining words makes a dimension on its own, the result of the Q-sort test delivers a total of 21 dimensions compared to 22 dimensions initially defined. In general, the two sets of dimensions are very similar and can be reconciled with minor adjustments described in the description of each dimension.

The application of the Q-Sort test consist on printed labels that reviewers spreaded on a table and bundled together with rubber bands. Reviewers were told to choose a word to put on top of each bundle of words as their choice of that dimension name. The word that is chosen more times by the reviewers is adopted as the dimension's name. As shown in the instructions of the Q-sort, reviewers could have chosen super categories where other categories were included. These super categories are also indication of the representativeness of the word as to be used as a dimension name. The basic practical framework is determined by the dimensions within which factors can be placed. The following is the final list of dimensions resulting from the reconciliation of the two sets of categories pre and post Q-sort test.

### DFR Dimensions

1. People

This is the dimension comprising those factors in which the subjects of the action or condition are users, customers, stakeholders, personnel, teams and people in general. There is a perfect match of the words included in this dimension between the researcher's categorization and the result of the Q-sort test. “People” is the most selected word as category or super category name (14 times).

2. Business

This is the dimension comprising those factors in which the subjects of the action or condition are the business, the organization or the corporation. There is a perfect match of the words included in this dimension between the researcher's categorization and the result of the Q-sort test. "Business" is the most selected name as category or super category (12 times).

3. Events

This is the dimension comprising those factors in which the subjects of the action or condition are events, incidents, targets, attacks, risks, intrusions, and threats. The researcher and the Q-sort test coincide in four words included in this dimension. A representative number of reviewers associated the words "event," "incident," and "target" with at least three of the others in the category. Therefore, their inclusion seems to be consensual. "Event" is the most selected name as category or super category (14 times).

4. Technology

This is the dimension comprising those factors in which the subjects of the action or condition are the hardware, the servers, the computers, the equipment, the network, the technology, and the technical issues. The researcher and the Q-sort test coincide in that the words computer, equipment, hardware, and server belong together. However, the pre Q-test classification had Tools as part of this category, and network and technology in different categories. Unlike the definition of technology as comprising hardware and software (Kroenke 2014), the reviewers did not include any of the words of the System category, where software is, at the levels of support and confidence expected. Likewise, the majority of reviewers did not include here the word "technical." The relationship between "technical" and "technology," though, shows up at the more lenient conditions of support 0.357 (9/252) and confidence 0.473 (9/19). Given that the pre Q-sort categorization also puts them together, "technical" is included in this category. As for the word "tools," the reviewers' choice is adopted. "Technology" is the most selected name as category or super category (13 times).

5. Information

This is the dimension comprising those factors in which the subjects of the action or condition are the information or the data. The initial category contained also "record" and "document," but the majority of reviewers see these two words as making a different category. "Information" is the most selected name as category or super category (12 times).

6. Document

This is the dimension comprising those factors in which the subjects of the action or condition are documents or records. Although the pre Q-test has these terms in the same category with "information" and "data," the reviewers seem to associate them more with the word "proof." This can be seen by creating a model in R with more lenient parameters (i.e., support = 0.357 or 9/252 and confidence = 0.473 or 9/19). At this level, a rule associating record and proof shows up ({Record} => {Proof} support = 0.03571429, and confidence = 0.4736842). Given this lack of agreement, this category will be kept as the majority of reviewers see it. "Document" is the most selected name as category or super category (2 times).

7. Evidence

This is the dimension comprising those factors in which the subjects of the action or condition are the proof, the demonstration, the case, the evidence or the chain of evidence. The pre Q-test has "demonstration" in the same category of "evidence" and "proof," but the majority of reviewers include the word "case" instead of "demonstration." Still, "demonstration" is by definition the action of giving proof or evidence, hence having it as an independent category would be redundant. Therefore, "demonstration" is included in this category as initially proposed. Likewise, "chain" is included in this category despite not being associated with any category by reviewers. The word "chain" is almost always used in the literature reviewed as "the chain of evidence;" hence, this is the natural category for it. "Evidence" is the most selected name as category or super category (13 times).

8. Environment

This is the dimension comprising those factors in which the subjects of the action or condition are the premises, the site, the space, the workspace, the lab, and the environment in general. The pre Q-sort test did not include "environment," but it included all other words in this category. The majority of reviewers, however, associate "environment" with "workspace," "space," and "site." Moreover, it was considered the most comprehensive term. "Environment" is the most selected name as category or super category (15 times).

9. Resources

This is the dimension comprising those factors in which the subjects of the action or condition are the assets, the tools or the resources in general. The category of "assets" and "resources" was predicted exactly as it was proposed by the majority of reviewers. The word “tools” is added because reviewers did not agree placing it in any other category, and it is generic enough to be understood as any helpful resource available. “Resource” is the most selected name as category or super category (21 times).

10. Infrastructure

This is the dimension comprising those factors in which the subjects of the action or condition are the architecture or the infrastructure. Both words were independent categories in the pre Q-sort test. The reviewers’ consensus is that they are together. “Infrastructure” is the most selected name as category or super category (6 times).

11. System

This is the dimension comprising those factors in which the subjects of the action or condition are the software, the program, the code, and the system. All words in this category were proposed in distinct groups in the pre Q-sort test. However, the majority of reviewers put them together with no overlapping with other categories at the levels of support and confidence assigned. “Software” and “system” are the most selected names as category or super category (7 times), but “system” is selected more times (3) as super category than “software” (1).

12. Methods

This is the dimension comprising those factors in which the subjects of the action or condition are the guidelines, the flow, the methods, the processes, the procedures, and the operations. “Policy” was associated with “procedures” by reviewers. However, it was also associated with two other words in a different category (rule and requirement), where it seems to fit better and agrees with the pre Q-sort classification. “Guideline” is also associated with “strategy” and “plan,” which belong to a different category. However, such an association has a weaker support than with “procedure.” Although the pre Q-sort classification assigned guideline to the Law category, the evidence post Q-sort test supports leaving it in the Methods category. “Method” is the most selected name as category or super category (13 times).

13. Law

This is the dimension comprising those factors in which the subjects of the action or condition are the law, the policies, the rules, and the requirements. “Policy” also shows up in the Methods category associated with “procedures.” However, it has a better fit in this category where it is associated with “rule” and “requirement” as in the pre Q-sort classification. On the other hand, “guideline” is also associated with “rule” and “policy.” However, such an association has a weaker support than with “procedure;” hence, although the pre Q-sort classification assigned “guideline” to the Law category, the evidence post Q-sort test supports leaving it in the Methods category. An additional consideration is that factors with the word “legal” are not filtered by the word “Law;” therefore, “legal” must be added as a selection criterion when adding indicators to the Law dimension. “Law” is the most selected name as category or super category (8 times).

14. Strategy

This is the dimension comprising those factors in which the subjects of the action or condition are the strategy, the plan, the tasks, and the objectives. A majority of reviewers also associated “guideline” with “strategy” and “plan,” but with a weaker support than the relation between “guideline” and “procedure.” The evidence post Q-sort test supports leaving it in the Methods category. “Task” is not supported by reviewers in any category. However, it was included in the initial classification and has a better fit in the Strategy dimension because strategic plans are deployed through tasks. “Strategy” is the most selected name as category or super category (10 times).

15. Miscellaneous

The words “cloud,” “time,” “external,” and “context” did not have support from a significant number of reviewers to share the same category with any other word. They will be put in a separate dimension where factors with unclear classification can be placed. This dimension is called miscellaneous in order to convey the idea that it is not associated with any particular entity, but with general aspects.

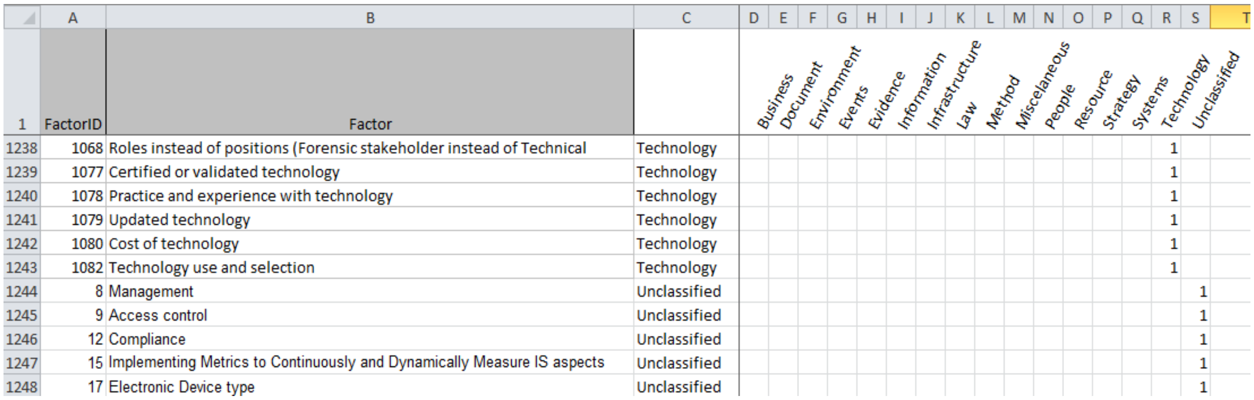
**Reduction of Indicators per Dimension**

After the dimensions are defined, items representing factors or indicators are assigned to dimensions. This is done, initially, by matching the words describing them with the words describing each dimension. A sparse matrix as the one used in R is created in Excel with the list of entities (e.i., word sets or dimensions) in the first row and the list of items (factors or indicators) in the first column, and filled with the formula: =IFERROR(IF(SEARCH(“Dimension Word Cell”,”Factor Cell”)>0,1,0),0),

If the item mentions the entity, the intersecting cell of item and entity displays a number one, otherwise, it displays a number zero “0”. A root word instead of the complete word is used in order to improve the recall of words derived from the entity. For example the root “spa” retrieves the word “spatial” associated to “space” whereas “space” would not. A drawback is that by using “spa” the formula also retrieves “Transparency” because “spa” is included in that word. Yet, it is better to have extra items that can be trimmed off later, instead of losing factors that can be important in shaping dimensions. It also does not happen often enough times to demand writing a more complex algorithm.

This matrix is loaded into MS Access in order to make selection queries for each dimension of the items including any of the words associated to that dimension; hence, obtaining the group of items by dimension. The fact that some items are listed in more than one dimension is acceptable and convenient because those factors/indicators must contribute relevant content to several dimensions. Other items are not listed in any of the dimensions because none of the words describing them is part of the words defining a dimension. This are classified as “Unclassified” factors/indicators.

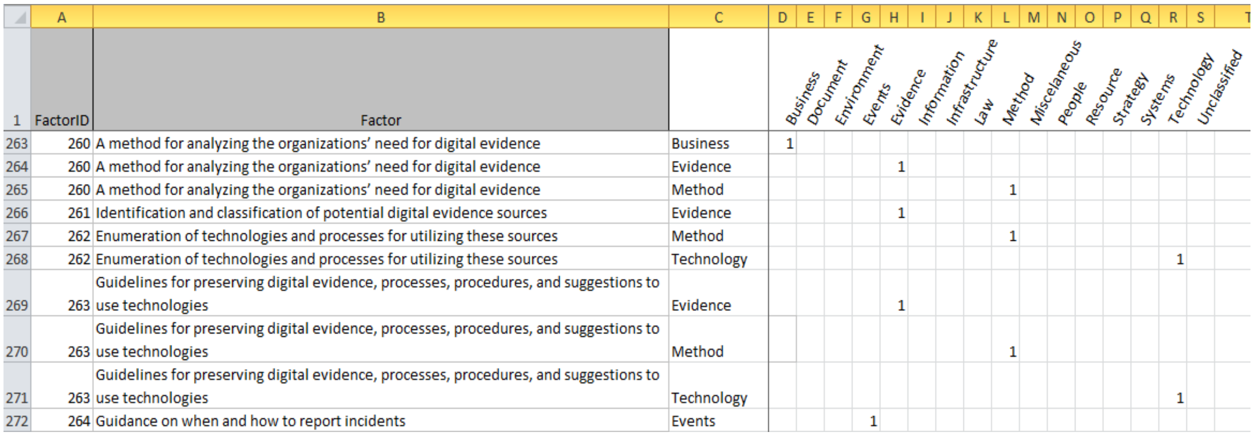
The complete list of items is sent back to Excel for further refinement. 1554 items are initially listed, including those unclassified and duplicated. This means that 439 items are duplicated factors. Before deleting repeated items, the list is transformed into a matrix by adding the dimensions in the first row. Each item is assigned a number one in its intersection with a column describing the dimension it belongs to, as shown below.



| | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | FactorID | Factor | | Business | Document | Environment | Events | Evidence | Information | Infrastructure | Law | Method | Miscelaneous | People | Resource | Strategy | Systems | Technology | Unclassified | |
| 1238 | 1068 | Roles instead of positions (Forensic stakeholder instead of Technical | Technology | | | | | | | | | | | | | | | 1 | | |
| 1239 | 1077 | Certified or validated technology | Technology | | | | | | | | | | | | | | | 1 | | |
| 1240 | 1078 | Practice and experience with technology | Technology | | | | | | | | | | | | | | | 1 | | |
| 1241 | 1079 | Updated technology | Technology | | | | | | | | | | | | | | | 1 | | |
| 1242 | 1080 | Cost of technology | Technology | | | | | | | | | | | | | | | 1 | | |
| 1243 | 1082 | Technology use and selection | Technology | | | | | | | | | | | | | | | 1 | | |
| 1244 | 8 | Management | Unclassified | | | | | | | | | | | | | | | | 1 | |
| 1245 | 9 | Access control | Unclassified | | | | | | | | | | | | | | | | 1 | |
| 1246 | 12 | Compliance | Unclassified | | | | | | | | | | | | | | | | 1 | |
| 1247 | 15 | Implementing Metrics to Continuously and Dynamically Measure IS aspects | Unclassified | | | | | | | | | | | | | | | | 1 | |
| 1248 | 17 | Electronic Device type | Unclassified | | | | | | | | | | | | | | | | 1 | |

Figure 5. Extract of the list of 1554 classified factors by dimension

In order to get rid of the duplicated items, the list is ordered by FactorID which is a key field used to uniquely identify each item; hence, the duplicated factors/indicators are easily spotted next to each other. Only one of the items is left in the list, preserving its association to all dimensions to which it was assigned. In the image below records 263 and 264 corresponding to FactorID 260 are deleted and record 265 remains with number ones marked in its intersections with business, evidence, and method. A list free of duplicates has 1115 items.

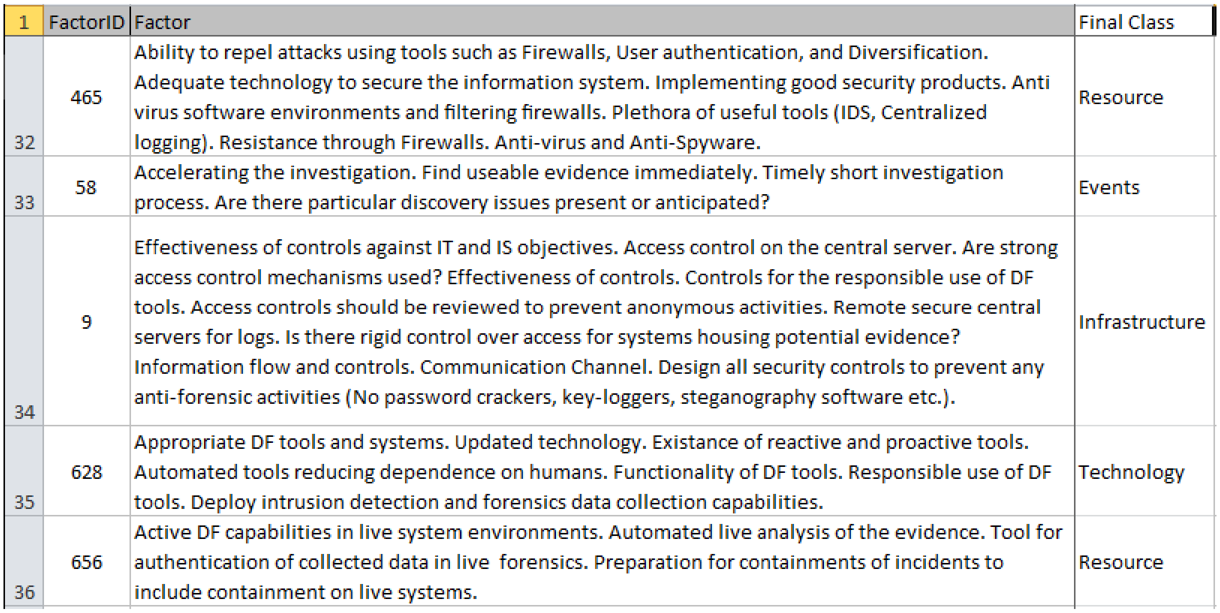


| | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | FactorID | Factor | | Business | Document | Environment | Events | Evidence | Information | Infrastructure | Law | Method | Miscelaneous | People | Resource | Strategy | Systems | Technology | Unclassified | |
| 263 | 260 | A method for analyzing the organizations’ need for digital evidence | Business | 1 | | | | | | | | | | | | | | | | |
| 264 | 260 | A method for analyzing the organizations’ need for digital evidence | Evidence | | | | | 1 | | | | | | | | | | | | |
| 265 | 260 | A method for analyzing the organizations’ need for digital evidence | Method | | | | | | | | | 1 | | | | | | | | |
| 266 | 261 | Identification and classification of potential digital evidence sources | Evidence | | | | | 1 | | | | | | | | | | | | |
| 267 | 262 | Enumeration of technologies and processes for utilizing these sources | Method | | | | | | | | | 1 | | | | | | | | |
| 268 | 262 | Enumeration of technologies and processes for utilizing these sources | Technology | | | | | | | | | | | | | | | 1 | | |
| 269 | 263 | Guidelines for preserving digital evidence, processes, procedures, and suggestions to use technologies | Evidence | | | | | 1 | | | | | | | | | | | | |
| 270 | 263 | Guidelines for preserving digital evidence, processes, procedures, and suggestions to use technologies | Method | | | | | | | | | 1 | | | | | | | | |
| 271 | 263 | Guidelines for preserving digital evidence, processes, procedures, and suggestions to use technologies | Technology | | | | | | | | | | | | | | | 1 | | |
| 272 | 264 | Guidance on when and how to report incidents | Events | | | | 1 | | | | | | | | | | | | | |

Figure 6. Extract of the list of reordered factors by FactorID to spot duplicates

There are also factors with very similar description and different FactorID. For example, training, training of personnel, and staff training may appear as independent factors while being semantically equivalent. Because only one is needed, duplicates must be eliminated. In order to refine the allocation of unclassified or misclassified factors, the items are reviewed one by one, and marked with ones in the dimensions where they can belong. By later applying a filter of items by dimension, semantically equivalent items can be spotted and reduced to a single one.

In addition, items addressing the same topic are grouped together for further elaboration of the appropriate questions. The figure below shows several items per cell separated by a period or a question mark. For example, row 32 groups several items under the FactorID 465 which together inquire about the organization’s ability to repeal attacks by implementing user authentication, firewalls and other technology resources. Likewise, row 33 groups items under the FactorID 58 inquiring about the organization’s ability to perform a fast investigation in the event of an incident.



| 1 | FactorID | Factor | Final Class |
|---|---|---|---|
| 32 | 465 | Ability to repel attacks using tools such as Firewalls, User authentication, and Diversification. Adequate technology to secure the information system. Implementing good security products. Anti virus software environments and filtering firewalls. Plethora of useful tools (IDS, Centralized logging). Resistance through Firewalls. Anti-virus and Anti-Spyware. | Resource |
| 33 | 58 | Accelerating the investigation. Find useable evidence immediately. Timely short investigation process. Are there particular discovery issues present or anticipated? | Events |
| 34 | 9 | Effectiveness of controls against IT and IS objectives. Access control on the central server. Are strong access control mechanisms used? Effectiveness of controls. Controls for the responsible use of DF tools. Access controls should be reviewed to prevent anonymous activities. Remote secure central servers for logs. Is there rigid control over access for systems housing potential evidence? Information flow and controls. Communication Channel. Design all security controls to prevent any anti-forensic activities (No password crackers, key-loggers, steganography software etc.). | Infrastructure |
| 35 | 628 | Appropriate DF tools and systems. Updated technology. Existance of reactive and proactive tools. Automated tools reducing dependence on humans. Functionality of DF tools. Responsible use of DF tools. Deploy intrusion detection and forensics data collection capabilities. | Technology |
| 36 | 656 | Active DF capabilities in live system environments. Automated live analysis of the evidence. Tool for authentication of collected data in live  forensics. Preparation for containments of incidents to include containment on live systems. | Resource |

Figure 7. Extract of the list of regrouped factors without semantic duplicates

Indicators grouped this way reduce the whole list to 148 Items throughout all dimensions. Because they still are independent phrases it is necessary to work on redacting specific phrases that can be put in a survey such that respondents can show their level of agreement with them. Redacting the items of the survey aims to identify the entities involved in the indicator, any relevant qualifying aspect of the entity (the type, the amount, etc.), the action that the entity exerts or that is exerted on the entity, and the attributes of such action that renders the factor measurable. As a result, each group of items can be represented by one or more questions.

After re-estructuring these phrases, the number of independent questions or usable indicators increases to 206. However, few of the independent questions coming from different groups of items were found similar, merged into one, and assigned to the most appropriate dimension leaving. Also, given the importance that authors give to awareness as a factor affecting DFR, two similar questions asking for the general perception of DFR are added at the beginning and at the end of the survey to test the impact of the survey as an instrument of awareness of DFR.

In total, 191 questions remain.

One more revision and adjustment is performed to assure that all rephrased questions are assigned to the dimension where they are most relevant. Provided that a professional is in charge of the assessment and detailed analysis of some of the items can be peformed in order to respond them, this detailed questionnaire classified by dimensions is a practical DFR framework that a practitioner can use to assess the level of DFR in an organization in a structural way. Most questions are stated such that they can be answered in terms of respondents' agreement with the assertion. Few remaining questions require numeric answers. When strong agreement or higher numeric value is associated to higher digital forensic readiness, this correlation is positive. The theoretical relationship between each item and the DFR status, as inferred from the literature review, is added in the column to the right of the table. In few cases, it is to the practitioner to decide whether the response is associated to more or less DFR. This questionnaire can also help a professional DFR specialist spot when perceptions of respondents do not match the reality of the readiness of their organization. Questions IDs are not consecutive because the list was alphabetically reordered by dimensions.

Table 10. Practitioners' DFR Framework

| QID | Question | Dimension | DFR Corr. |
|---|---|---|---|
| 1 | Industry sector of the organization. | Business | Depends |
| 2 | Organization size in sales. | Business | Negative |
| 3 | Organization size in number of employees. | Business | Negative |
| 4 | Organization size in number of customers. | Business | Negative |
| 5 | The organization has a forensic culture of preserving evidence, following digital evidence preservation processes, and acquiring and sharing knowledge in computer security and digital forensics. | Business | Positive |
| 6 | The organization has a corporate culture of secrecy such that proactive forensics activities are kept from users and few staff knows detailed security information. | Business | Negative |
| 7 | The organization has a reputation of back-tracking intruders and assessing their danger to society. | Business | Positive |
| 8 | Management is convinced of the importance of digital forensic readiness (e.g., they show support, provide governance, and assume full commitment, responsibility and accountability towards the forensic program). | Business | Positive |
| 9 | Implementing a digital forensics program is expensive. | Business | Negative |
| 10 | This organization is exposed to many risks and threats. | Business | Positive |
| 11 | Our firm has a public profile therefore protecting its reputation and image is a corporate objective. | Business | Positive |
| 12 | This organization has a high number of locations. | Business | Negative |
| 41 | The organization has a quality assurance system that covers policies, activities, procedures, documentation, and management thereby ensuring consistency, efficiency and transparency of technical and non-technical business processes. | Business | Positive |
| 42 | The organization funding for digital forensic readiness (i.e., collection, analysis and preservation of digital evidence) is sufficient. | Business | Positive |
| 43 | The organization uses computer forensics to seek legal accountability for intruder behavior. | Business | Positive |
| 44 | IT security and digital forensics governance programs, policies, services, and procedures are mature enough to guarantee confidentiality, integrity, availability, authentication and non-repudiation of information. | Business | Positive |
| 45 | IT security and digital forensics governance programs, policies, services, and procedures guarantee adequate management, skills, and resources to determine the source of an attack and the recovery of digital evidence. | Business | Positive |
| 40 | Given the definition of digital forensic readiness (DFR) as the state of preparedness to obtain, understand, and present verifiable digital evidence when needed, I would rate my organization's DFR as high. | Business | Depends |
| 191 | After completing this survey and given the definition of digital forensic readiness (DFR) as the state of preparedness to obtain, understand, and present verifiable digital evidence when needed, I would rate my organization's DFR as high. | Business | Positive |
| 46 | The system security architecture is documented. | Document | Positive |
| 47 | The organization has an asset registry for items of electronic equipment that could record information. | Document | Positive |

| | | | |
|---|---|---|---|
| 48 | The organization has a documented and validated investigation protocol guided by best practices. | Document | Positive |
| 49 | The organization has an archive of the organization’s incident, crime and dispute history identifying each case, date, impact, entry point of attack, security measures in place at the moment, suspected causes that allow the incident to occur, who knew what about the attack and when they knew it, investigative digital forensic team rosters and roles, descriptions of incident responses and errors, and technical and non-technical issues affecting the success or failure of the attack. | Document | Positive |
| 50 | The organization has reports on the lessons learned from incidents, including success in dealing with and recovering from the incident, what could have been done differently if the scenario had occurred on a different day or at a different time (regular hours versus off-hours) or at a different physical location (onsite versus offsite). | Document | Positive |
| 51 | The organization keeps records of user behavior with network-based applications and documents anomalous observations. | Document | Positive |
| 52 | The organization maintains a database of file hashes for common operating system files and for deployed applications, using file integrity checking software on important assets. | Document | Positive |
| 53 | The organization maintains a change management database. | Document | Positive |
| 54 | The organization maintains documented records (e.g., baselines) of network and system configurations. | Document | Positive |
| 55 | The organization has a secure location for logs storage that also stores meta-data, such as author and date, with the record. | Document | Positive |
| 56 | The organization stores records about training, procedures, people, roles, and policies. | Document | Positive |
| 13 | The organization provides security wizards for safe conduct within the workspace environment. | Environment | Positive |
| 14 | The organization can safely and effectively control and document the scene of a digital forensic incident. | Environment | Positive |
| 15 | The organization can conduct an onsite examination without affecting the integrity of the original evidence. | Environment | Positive |
| 16 | The location of the organization makes it insecure. | Environment | Negative |
| 57 | Physical access to work sites and to the perimeter of any premises that contain servers are controlled and secured with security technologies such as physical access control, location sensors, and closed-circuit television (CCTV). | Environment | Positive |
| 58 | The organization's forensic laboratories are accreditated and frequently audited. | Environment | Positive |
| 59 | Computer forensic examiners in the organization have a proper laboratory, equipment, hardware and software for onsite examinations. | Environment | Positive |
| 60 | The organization has multiple virtual locations, wired and wireless networks, and/or a mobile platform. | Environment | Negative |
| 17 | In case of a cyber incident, the organization's personnel have clear criteria on whether or not they should turn off a hacked system or device. | Events | Positive |
| 18 | The organization knows how to handle a politically sensitive or publicly embarrassing incident. | Events | Positive |
| 61 | The organization automatically preserves evidence related to a suspicious event, via hashing, in case of an incident. | Events | Positive |

|  |  |  |  |
|---|---|---|---|
| 62 | In case of a cyber incident, the organization will be able to assess the impact on stakeholders and to propose forensic analysis hypotheses that will help identify potential charges. | Events | Positive |
| 63 | In case of a cyber incident, the organization knows which forensic tools and techniques it needs to deploy. | Events | Positive |
| 64 | In case of a cyber incident, the organization knows where to look in the system in order to identify case specific evidence supported by event log information and Internal integrity checks. | Events | Positive |
| 65 | In case of a cyber incident, the organization can anticipate its discovery needs and accelerate its investigation to find timely and useable evidence. | Events | Positive |
| 66 | The organization is able to forecast and control the escalation of costs when facing a digital forensic incident. | Events | Positive |
| 67 | In case of a cyber incident, the organization is able to determine whether a warrant allows for an onsite or in situ examination, seizure and removal of the system(s). | Events | Positive |
| 68 | In case of a cyber incident, the organization will be able to recognize the range of personnel within the firm who may be involved in a legal inquiry. | Events | Positive |
| 69 | In case of a cyber incident, the organization will be able to determine the remoteness of the crime by identifying remote web access and establishing the location of the network intrusion detection system relative to an intruder. | Events | Positive |
| 70 | In case of a cyber incident, the organization will be able to determine the time, timeline of events, and duration of the incident. | Events | Positive |
| 71 | In case of a cyber incident, the organization will be able to determine the nature of the incident, the type of case, and the crime category. | Events | Positive |
| 72 | In case of a cyber incident, the organization can determine the technical skill and knowledge level of the suspect. | Events | Positive |
| 73 | In case of a cyber incident, the organization is able to determine what IT systems and types of technologies were involved, such as standalone systems, complex networks, multi-user systems, etc. | Events | Positive |
| 74 | The organizational plan of incident response incorporates policies, procedures, personnel assignments, and/or technical requirements to mitigate risk and prepare for events requiring digital forensic intervention. | Events | Positive |
| 75 | The incident response plan of the organization correlates events with an established Bayesian network, determines critical response times, and specifies when to activate the Disaster Recovery Plan (DRP) and the Business Continuity Plan (BCP). | Events | Positive |
| 76 | The organization applies an algorithm to assess evidence value by considering its nature (content or metadata), evidencial weight (completeness and admissibility), its temporal value (MAC times, cookies, cache and the index.dat file), its exposure and risk, and the cost/benefit of its retrieval.. | Evidence | Positive |
| 77 | The organization knows what information in what format is required as evidence in a civil litigation or criminal proceeding as well as how to use it to determine the root cause of an event. | Evidence | Positive |
| 78 | The organization has a plan to prepare, map, store, transport, control access to, and present evidence, preserving its integrity and ensuring it makes a positive impact on the outcome of any legal action. | Evidence | Positive |

| | | | |
|---|---|---|---|
| 79 | In case of a cyber incident, the organization can provide detailed log and documentation of the chain of evidence at every step (e.g. data collection, storage, examination, handling) which can demonstrate the authenticity, credibility, and reliability of electronic evidence, including information about the tools used. | Evidence | Positive |
| 80 | The organization has identified, classified, and prioritized the sources and types of potential evidence by considering the legality and cost-effectiveness of the collection process, alternative evidence sources, and the potential for escalation into formal investigations involving law enforcement agencies. | Evidence | Positive |
| 81 | The organization employs encryption standards and cryptographic hashes for evidence files. | Evidence | Positive |
| 106 | The organization applies a proportionality rule to collect only useful evidence upon good cause and balances liability vs. obligation in the retention of log data. | Evidence | Positive |
| 82 | The amount of data produced in the organization every month is high. | Information | Positive |
| 83 | The organization knows the sources and format of its data, when and where data is generated, the associated threats to the data, and how data is preserved for long-term storage. | Information | Positive |
| 84 | The organization requires network activity logs that lists date, time, and user stamps for all files, and triangulates logs with other data (e.g., timing of links, CCTV pictures, user identification records, etc.) to be able to guarantee internal integrity of authentication logs in client and server computers and prove timeline and association of data to metadata, including cloud-based resources. | Information | Positive |
| 85 | The organization uses statistical interpretation, data mining, filtering techniques and pattern matching to find digital evidence. | Information | Positive |
| 86 | The organization formats log data in a single format, such as syslog. | Information | Positive |
| 87 | The organization keeps data regarding the state of the file system, patterns of physical traces and imprints (i.e., logs, audits, what is logged, and how logging is done). | Information | Positive |
| 20 | Wireless access is allowed in the organization. | Infrastructure | Negative |
| 88 | The organization mantains effective controls on information flow and channels (including remotely located logs) to prevent anonymous activities, access to central servers and systems housing potential evidence, access to digital forensics tools, and anti-forensic activities (e.g. password crackers, key-loggers, steganography software etc.). | Infrastructure | Positive |
| 89 | The digital and physical infrastructure and architecture have been developed with embedded forensic capabilities in networks and computing platforms such that all authentication attempts are recorded, applications perform auditing, the design is fault tolerant, and the architecture facilitates recovery. | Infrastructure | Positive |
| 90 | The organization's systems security architecture configuration follows consistent standards throughout the entire platform. | Infrastructure | Positive |
| 91 | The organization implements endpoint security in order to maintain control over its data and decrease access to forensic data. | Infrastructure | Positive |

| | | | |
|---|---|---|---|
| 92 | The organization routinely evaluates Internet activities (cookies, temporary files, URLs, email, instant messages), checks for gaps in the SMTP send-receiver pairs, acknowledges packet protocols, and monitors interactions between network applications and the traffic they generate. These monitored interactions include layer 7 of the OSI model (e.g. static and dynamic web applications, web clients, web servers, application servers and web services). | Infrastructure | Positive |
| 93 | The organization implements multitiered logging. | Infrastructure | Positive |
| 94 | The organization has centralized logging and data, thus audit records are forwarded to secure centralized log servers. | Infrastructure | Positive |
| 95 | Logging features are architected to support effective incident response. | Infrastructure | Positive |
| 96 | The organization implements strong user authentication and role based access control with the least privilege principle in mind and with separate life-cycle related logs per user. | Infrastructure | Positive |
| 97 | Strong two-factor authentication is required to access all critical systems. | Infrastructure | Positive |
| 98 | The organization implements defined procedures and public key infrastructure (PKI)  system architecture where log files relating to access (log-in, access to all files) are separated from PKI services-related logs. | Infrastructure | Positive |
| 99 | Logs are shared across institutional boundaries. Information is kept in several repositories to minimize impact in case of loss of data. | Infrastructure | Positive |
| 100 | The organization’s IT infrastructure is monitored using intrusion detection systems (IDS), antivirus software, and spyware detection and removal utilities in servers, workstations, removable/portable devices, and network devices/activities (e.g. log network and host activity). This monitoring distinguishes between hardware and software and considers trade-offs involving IDS monitoring and reporting. | Infrastructure | Positive |
| 101 | Digital forensic tools are used for non-forensic purposes to enhance the organization's security architecture, for example to recover lost data. | Infrastructure | Positive |
| 102 | The organization's wireless infrastructure is kept secure. | Infrastructure | Positive |
| 21 | The organization has policies defining a point of contact with authorities and how communications with external parties (e.g. stakeholders, law enforcement, ISPs) might occur, particularly with regard to emerging issues, potential risks, investigation results, and evidence release. | Law | Positive |
| 22 | The organization has policies clarifying consent of monitoring without expectation of privacy/ownership of data by employees, and conditions for Bring Your Own Device (BYOD) practices. | Law | Positive |
| 23 | The organization has policies clarifying its ownership of data and use of information systems resources by members of the organization, including data storage in personal devices with specific directives governing device type and the use of small/easy to hide devices. | Law | Positive |
| 24 | The organization has policies defining business scenarios that require digital evidence, what information must be preserved under certain circumstances and for how long, its accessibility, and the conditions necessary to destroy it without losing history, in compliance with records legislation. | Law | Positive |

| | | | |
|---|---|---|---|
| 25 | The organization has policies that disallow the use of its intranet when handling digital evidence. | Law | Positive |
| 26 | The organization has corporate security policies that govern digital assets, forensic events, data collection/storage, preventive security, and codes of conduct. | Law | Positive |
| 27 | The organization implements measures to enforce forensic policies and make staff accountable of their digital forensic responsibilities. | Law | Positive |
| 28 | The organization has policies establishing the need for compliance with the regulatory framework of fiduciary, statutory and/or governmental regulations, even in the absence of forensic incidents (e.g. Sarbanes–Oxley, HIPAA, and penalties for security incidents). | Law | Positive |
| 29 | The organization's policies on information systems monitoring are consistent with its personnel privacy policies and applicable employment law. | Law | Positive |
| 103 | Safeguards for sensitive information and measures for handling inadvertent exposures are implemented. | Law | Positive |
| 104 | Disk scrubbing tools, file shredding software, personal file encryption, and anti-forensic strategies (e.g. anonymous activities, data destruction/alteration, and onion routing) are banned. | Law | Positive |
| 105 | The organization has policies defining types of risks, information retention requirements, security countermeasures, resourcing, intelligence, trigger events for internal investigation, when external professional or formal investigation is required, and the actions that may be taken | Law | Positive |
| 107 | Organization policies define the legal and managerial authority required for search and examination during ongoing investigations to ensure compliance with information security and regulatory requirements (e.g. rules of evidence for admissibility, 4th Amendment issues, litigation holds, and timely reporting obligations to a judge). | Law | Positive |
| 108 | The organization has a suspicion policy used to continually review potential sources of attacks or failure, complaints, potential crimes and disputes, and threats from opportunists, criminals, competitors or disgruntled employees. This policy indicates what evidence of an attack would look like and how to manage people leaving the company. | Law | Positive |
| 109 | The organization has policies for the specific jurisdictional requirements of countries where it has an operating presence and offers guidance on other industry-specific and multi-jurisdiction conditions regarding admissible evidence. | Law | Positive |
| 110 | The organization has policies on roles and responsibilities of all people and external organizations involved in digital forensic investigations, as well as separate policies for those involved in preserving, maintaining, and examining evidence (e.g., response/investigative teams and security personnel). | Law | Positive |
| 111 | The organization has received legal advice and review of forensic policies and high-level procedures regarding privacy, subpoenas, warrants, admissibility, data protection, human rights, limits to surveillance, obligations to staff members and others, disclosure in legal proceedings, and legal requirements and constraints on collection and preservation of potential digital evidence. | Law | Positive |

| | | | |
|---|---|---|---|
| 30 | The organization has a broad and complete digital forensics model defining the standardized phases (capture, store, analyze, preserve, integrate, and present evidence) of the response and investigation process. | Method | Positive |
| 112 | The organization conducts regular compliance reviews and updates its policies, procedures, and organizational memory according to changes in risk assessment, the legal framework and/or organizational requirements (e.g. moving to the cloud). | Method | Positive |
| 113 | The organization has formal incident response procedures describing the trigger events to start active monitoring and systematic gathering of potential digital evidence (including pre-incident data collection), first response guidelines to preserve evidence, when and how to report incidents, how to choose an investigation model, and how to set action plans. | Method | Positive |
| 114 | The organization has formal procedures describing packaging, transportation, storage, handling, and preservation of physical and digital evidence. | Method | Positive |
| 115 | The organization has archive management procedures to assure that records (including those in the cloud) possess content, context and structure, while preserving evidence quality in terms of authenticity, reliability, integrity, and usability. | Method | Positive |
| 116 | The organization has formal procedures to assess its needs for digital evidence according to its risk assessment practices and its regulatory/legal framework. | Method | Positive |
| 117 | The organization has procedures (e.g., penetration tests, probes, audit analysis of server and network logs, and alerts from incidents detection/deterrence systems) describing the configuration and use of active monitoring and logging mechanisms to continually detect and deter incidents in system activities and electronic communications, including procedures to prevent alteration of intercepted communications. | Method | Positive |
| 118 | Forensic techniques are embedded in the organization's regular information management audits. | Method | Positive |
| 119 | Information security audit procedures follow standards, guidelines, and best practices that include protection of IT and business systems, monitoring of the forensics process, and patch management. | Method | Positive |
| 120 | The organization has reliable procedures for gathering admissible post-incident evidence which include: how to discover hidden data, weighed criteria that guide the collection of evidence based on storage volatility, sampling & reduction techniques, verifying the integrity of the data, and how to store and manipulate data. | Method | Positive |
| 121 | The organization has a formal unbiased procedure for examination of post-incident digital and physical evidence without modifying it. It includes choosing a forensic investigation model, a triage/prioritization model for analysis and interpretation by selecting which data source to check first and why, and managing all of the tasks in the investigation process. | Method | Positive |
| 122 | The organization has procedures for performing regular and sporadic backup of systems (e.g. imaging a hard disk, capturing volatile information or securing physical evidence), ensuring the use of hashing functions during evidence acquisition, and retaining backups for a specific period of time to facilitate recovery. | Method | Positive |

| | | | |
|---|---|---|---|
| 123 | The organization has policies and procedures guiding reasonable and appropriate use of forensic tools. | Method | Positive |
| 124 | The organization has procedures for performing RAM forensics and the collection of volatile data in the order of volatility and priority that are related to a specific organizational requirement and that deal with the forensic blurriness affecting fidelity and quantity of evidence acquired in live digital forensics. | Method | Positive |
| 125 | The organization can demonstrate due diligence and compliance with the organization''s policies and all applicable laws and regulations in all phases of a forensic investigation process. | Method | Positive |
| 126 | The organization has a formal process for the selection, use, testing, and maintenance of technology deployed in the organization's information systems, including the test and calibration of evidence collection devices and specifying their frequency of calibration. | Method | Positive |
| 127 | The organization's forensic procedures have been reviewed by experts and/or published in peer reviewed articles. | Method | Positive |
| 128 | The organization's forensic procedures are accepted within the relevant scientific community. | Method | Positive |
| 129 | The organization's forensic procedures have known error rates. | Method | Positive |
| 130 | The organization's forensic procedures state that the Daubert test will be applied to any expert testimony. | Method | Positive |
| 131 | The organization's forensic procedures have been tested and are kept up to date. | Method | Positive |
| 19 | In our organization, the forensic incident handlers do a good job of collecting evidence about compromised systems. | People | Positive |
| 31 | The organization's non-IT staff has substantial training in digital forensics; they understand forensics technologies and have practical experience with them. | People | Positive |
| 32 | The organization's personnel is committed to the forensics program; they see the tangible/intangible benefits of technologies such as anti-spyware. | People | Positive |
| 33 | Self-education on new forensic technologies is common among personnel in the organization. | People | Positive |
| 34 | The organization's employees have knowledge of information management. | People | Positive |
| 35 | Employees have digital forensic skills. | People | Positive |
| 36 | The organization's staff learns effectively from previous incident response experiences. | People | Positive |
| 37 | Employees understand the organization's security policies. | People | Positive |
| 132 | The organization has identified and developed the technology and personnel computing expertise to perform computer and network forensics and manage legal evidence properly. | People | Positive |
| 133 | The organization has a multi-disciplinary forensic response/investigative team, involving legal, IT, law enforcement, business, and auditing representatives, ready to work collaboratively on assigned roles in case of a cyber incident. | People | Positive |
| 134 | The organization's multi-disciplinary forensic response/investigative team is internal rathern than external. | People | Positive |
| 135 | Investigators who are members of the forensic team have education and certifications in digital forensics. | People | Positive |
| 136 | Information security auditors' assessment produces confidence in the security system. | People | Positive |

| | | | |
|---|---|---|---|
| 137 | The organization identifies and profiles system use, users, suspects, attackers, and victims at risk through: (1) ID management, (2) authorization and authentication credentials, (3) accesibility, responsibility, and ownership of data and financial instruments, and (4) personal information in data. | People | Positive |
| 138 | The organization monitors user behavior by tracing back the actions of each employee and retaining application and local user files (e.g. home directory, file properties, registry, profiles, and signatures). | People | Positive |
| 139 | The organization uses keystroke monitoring on its computers. | People | Depends |
| 140 | The organization traces custody of an individual's devices for upgrades and change of office or role. | People | Positive |
| 141 | The organization's investigators' background is more scientific than practical. | People | Depends |
| 142 | Interactions among the organization's forensic staff, other personnel, and external institutions involved in forensics or security processes flow smoothly based on mutual trust. | People | Positive |
| 143 | Staff members have a strong understanding of the organization's security policies. | People | Positive |
| 144 | The organization has the expertise and capabilities to distinguish anomalous events or criminal activities from normal operational activities. | Resource | Positive |
| 145 | The organization has the ability to repel attacks using tools such as firewalls, user authentication, and diversification. | Resource | Positive |
| 146 | The organization has active digital forensic capabilities in live system environments including automated live analysis, authentication of collected data, and containment of incidents. | Resource | Positive |
| 147 | Corporate physical and digital assets are classified and controlled considering their value, data linked to them, and likelihood of being targeted. | Resource | Positive |
| 148 | The organization has the technology (e.g. relevant software and automated tools) and human capacity to capture all types of communications and store, analyze, preserve, integrate, secure, and present admissible evidence in order to hold intruders accountable in a court of law, and pursue legal remedies. | Resource | Positive |
| 149 | The organization lists the technologies and processes needed for the forensic readiness program, and coordinates the deployment of these resources. | Resource | Positive |
| 150 | The organization has forensic toolkits that each include a hardware write blocker, e-camera, gloves, forms, supplies, etc. | Resource | Positive |
| 151 | The organization removes or relocates critical assets for better management and implementation of the forensic program. | Resource | Positive |
| 152 | The organization possesses and implements updated techniques and automated tools to investigate anti-forensics methods. | Resource | Positive |
| 153 | The organization has the ability and resources to recreate the investigated environment. | Resource | Positive |
| 154 | The organization has sufficient decryption capabilities to counter the increasingly pervasive use of encryption technologies. | Resource | Positive |

| | | | |
|---|---|---|---|
| 38 | The organization offers personnel and IT staff standardized training and certification programs in digital forensics including information security awareness, sensitivity of evidence, how to recognize and respond to an incident, roles and legal aspects of the digital evidence process, latest threats, use of IT and forensic tools, forensic policies' content, forensic examination, best practices in information security, and proper staff incident response behavior. | Strategy | Positive |
| 155 | The organization calculates the cost-benefit of collecting and analyzing digital evidence by weighing benefits against threats and risks, internal vs outsourcing costs, and return on security investment (ROSI). | Strategy | Positive |
| 156 | The organization performs a risk assessment considering vulnerabilities, threats, unknown risks, level of digital evidence exposure to threats, potential loss, cost of measures and threats, and benefit of measures. | Strategy | Positive |
| 157 | The organization provides appropriate ongoing training opportunities to managers, internal investigators, and members of the Computer Incident Response Team (CIRT). | Strategy | Positive |
| 158 | The organization has a business continuity plan to minimize interruption to the business while gathering admissible evidence, to provide or restore essential services during an attack, to avoid financial loss, and to recover assets using replication or backup. | Strategy | Positive |
| 159 | The impact of the implementation of digital forensic readiness in network operation, architecture, transmission frequencies, power consumption, overhead or sensitivity has been high. | Strategy | Negative |
| 160 | Corporate policies and procedures are developed collaboratively using collaboration tools to maintain a shared workspace. | Strategy | Positive |
| 161 | The organization prioritizes roles over positions, differentiates information management from systems/technology management, and segregates duties of digital forensics and information security teams. | Strategy | Positive |
| 162 | The organization has dedicated roles relating to security and forensics, such as team leader, incident investigator, digital forensics specialist, work space administrator, security/system administrator, security/system architect, prosecutor, law enforcement executive, point of contact/media liaison, and legal adviser. | Strategy | Positive |
| 163 | The corporate information security best practices include collection and preservation of potential digital evidence. | Strategy | Positive |
| 164 | The corporate governance model development process was informed by a well-developed forensic readiness policy. | Strategy | Positive |
| 165 | The organization's information systems development life cycle (ISDLC) includes collection and preservation of potential digital evidence. | Strategy | Positive |
| 166 | The organization understands digital forensics training requirements and encourages both formal and informal learning. | Strategy | Positive |
| 167 | The organization looks for external policies, regulations, legislation and recommendations to shape its policies, prevent incidents, and implement control practices, countermeasures, and risk management. | Strategy | Positive |
| 168 | The organization follows best practice security standards that have been validated by an international information security certification process. | Strategy | Positive |

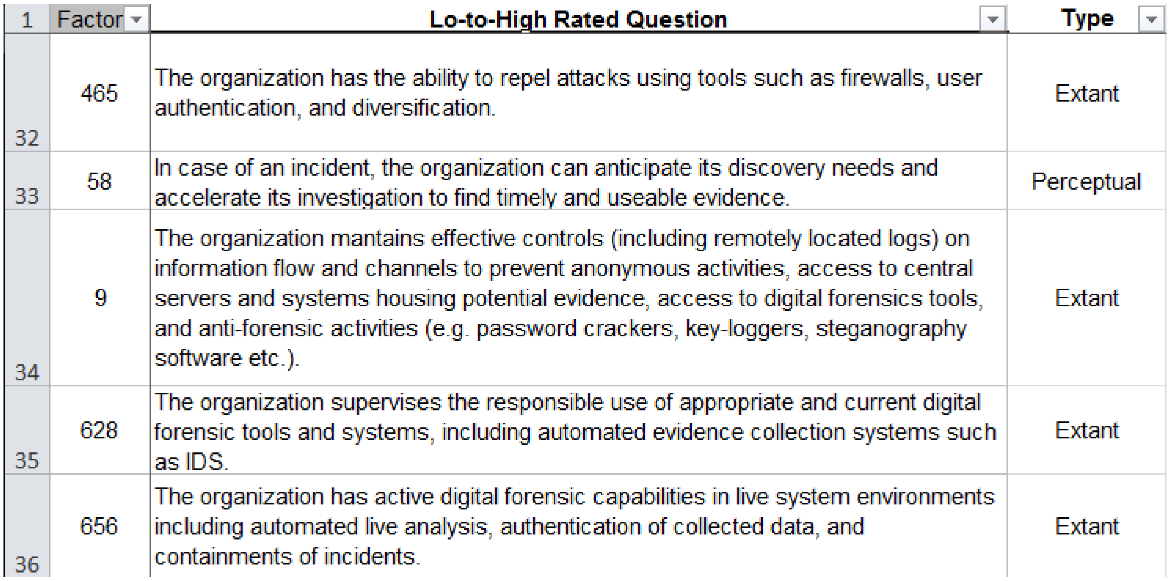
| | | | |
|---|---|---|---|
| 169 | The organization controls security information through dashboards and metrics that continuously and dynamically measure information security performance. | Strategy | Positive |
| 170 | The organization uses an external company such as an Independent Center for Incident Management (ICIM) to perform forensic analysis but has internal triaging capabilities. | Strategy | Positive |
| 171 | The organization manages external digital forensic investigators, establishes their capabilities and response times, and validates the accreditation of their laboratories. | Strategy | Positive |
| 172 | The organization participates in Information Sharing and Analysis Centers (ISACs). | Strategy | Positive |
| 173 | The organization's risk assessment process evaluates potential losses, classifies digital evidence exposure correlated with threats, checks security through audits, calibrates audits, and revisits residual risks after controls are implemented. | Strategy | Positive |
| 174 | The organization knows and adopts standards of the digital forensics discipline, including automated practices, and strives to monitor emerging academic digital forensics research. | Strategy | Positive |
| 175 | The organization performs security benchmarking to assess the preparedness of competitors and enemies. | Strategy | Positive |
| 176 | The organizational structure (e.g rank hierarchy, privileges, and roles and responsibilities model) has been designed or reviewed with consideration given to digital forensics needs. | Strategy | Positive |
| 177 | Information technology and information security objectives are aligned with the business mission and objectives. | Strategy | Positive |
| 178 | The organization's privacy policy and controls are aligned with the objectives of the digital forensics readiness program (e.g. compliance with regulation & legislation, internal investigation, forensic response, and legal evidence management). | Strategy | Positive |
| 179 | Fulfilling the demands that the legal system makes about admissibility and reliability of digital evidence for our organization is difficult. | Strategy | Negative |
| 180 | Our organization needs to produce reliable evidence: | Strategy | Positive |
| 39 | The organization's security system is reliable. | Systems | Positive |
| 181 | The organization possesses automated systems, such as intrusion detection systems, which provide alarms upon detection of potential incidents and provide reports to track incidents and perform audit trails. | Systems | Positive |
| 182 | The organization implements tamper-proof mechanisms for its systems. | Systems | Positive |
| 183 | The organization's security configuration provides hardware independence from operating systems. | Systems | Positive |
| 184 | The organization uses security event management software (SEM) or incident management software with an event triggering function. | Systems | Positive |
| 185 | All relevant devices and systems in the organization are synchronized with logging time recorded according to time-zones. | Systems | Positive |
| 186 | Information systems -- including operating systems, hardware, and software applications -- are properly configured for security. | Systems | Positive |
| 187 | The organization supervises the responsible use of appropriate and current digital forensic tools and systems, including automated evidence collection systems such as IDS. | Systems | Positive |

|  |  |  |  |
|---|---|---|---|
| 188 | The organization uses imaging technologies with lossless compression and hashing functions to preserve forensic evidence. | Technology | Positive |
| 189 | The organization's technology -- such as hardware, software, and forensic tools -- has been certified or validated. | Technology | Positive |
| 190 | The organization's storage technology is appropriate in capacity and functionality, including storage visualization abilities. | Technology | Positive |

**Higher Level Questionnaire**

Because it will probably demand considerable time and knowledge for an individual respondent to complete this questionnaire, a higher-level questionnaire is developed to perform exploratory factor analysis and develop a statistically supported framework of DFR. While the dimensions previously developed are useful to define the practitioners’ DFR framework and facilitate the reduction of the number of indicators, a conceptual model requires a different approach where the indicators are grouped according to their mutual, or lack of it, correlation. It is also important to note that items distilled from the literature may comprehend both formative and reflective indicators. Therefore, it is necessary to make this distinction.

Based on the definition of formative and reflective indicators, this research considers formative those factors adding up to a better status of DFR, while deeming reflective those which are a perception of respondents. In the first case, the respondent simply acknowledges a reality, whereas in the second he/she gives his/her opinion. Figure 8 shows an extract of this classification as extant or perceptual indicators, using factors 465, 58, 9, 628, and 656, previously presented in Figure 7.



| 1 | Factor | Lo-to-High Rated Question | Type |
|---|---|---|---|
| 32 | 465 | The organization has the ability to repel attacks using tools such as firewalls, user authentication, and diversification. | Extant |
| 33 | 58 | In case of an incident, the organization can anticipate its discovery needs and accelerate its investigation to find timely and useable evidence. | Perceptual |
| 34 | 9 | The organization mantains effective controls (including remotely located logs) on information flow and channels to prevent anonymous activities, access to central servers and systems housing potential evidence, access to digital forensics tools, and anti-forensic activities (e.g. password crackers, key-loggers, steganography software etc.). | Extant |
| 35 | 628 | The organization supervises the responsible use of appropriate and current digital forensic tools and systems, including automated evidence collection systems such as IDS. | Extant |
| 36 | 656 | The organization has active digital forensic capabilities in live system environments including automated live analysis, authentication of collected data, and containments of incidents. | Extant |

Figure 8. Extract of list of extant and perceptual questions

The higher level questionnaire reduces the length and amount of questions by omitting lower-level details associated to some questions. For example, instead of asking whether the organization has a laboratory with proper tools and technologies (item 59), whether such laboratory is certified and frequently audited (item 58), and whether its technology has been validated (item 189), a higher-level question simply asks about the existence of the laboratory and the forensic tools. The certification and validation of the laboratory and tools are at a deeper level of specialization in DFR that is not expected from most organizations at this moment. If having a laboratory and tools for forensic investigation turns out to be a good predictor of the forensic preparedness then further assessment should investigate more specific conditions of those tools and laboratory.

Another characteristic of the higher-level questions is that they can be classified in one of five subtypes. It can be seen that most items refer to something that the organization has, something that it does or something that it knows. Few remaining items are demographic characteristics of the firm or a respondent's perception of an organizational situation. Therefore, we can name the subtypes as: demographic, has, does, knows, and perceived. This reordering facilitates respondent's understanding of the questions.

Most questions are Likert-type questions. Few other questions are Yes/No or ranges, and when possible, semantic differential scales are used because they yield the same statistic results, increase nomological validity and reduce time response (Chin, Johnson & Schwarz 2008). In order to make it easier for respondents to identify the subject of the questions, each specific group has one general introduction. Therefore, respondents know that all items below refer to a "has", "does", "knows" or "perception" of the organization. Although most "demographics", "has", "does", and "knows" questions correspond to the originally labeled extant indicators, there are few exceptions. For example, while the higher-level questionnaire asks whether the firm "has" a culture of secrecy, the researcher reads this as a perceptual question based on the judgement of the respondent. The same happens with several "knows" questions because whether the firm knows something or not is decided by the respondent's perception.

On the contrary, it is more unlikely that something that the respondent acknowledges as existing in, or being performed by the organization, is simply a matter of opinion. In general, questions move from extant to perceptual in the following order of subtypes: demographics, has, does, knows, perceived. The list of the 76 higher-level questions is attached as Appendix E and presents items subtypes, a new ID identifier per question, and the items from the detailed questionnaire that are covered by each item of the higher-level questionnaire, to facilitate back tracking.

### Factor Analysis

Exploratory factor analysis (EFA) is performed on the extant and perceptual factors first in a pilot study and later on the final study. Given that factor analysis can be used as a clustering technique to group respondents, let us make clear that the objective of this EFA is to group variables and not respondents.

For the perceptual factors, this research uses maximum likelihood as the extraction method, thus assuming that these factors are a reflection of the real DFR status. As for the extant factors, these are considered formative of the DFR construct; therefore, they are treated as components, and the principal components extraction method is used in this case. In the pilot study, both extractions were done using SPSS with the orthogonal varimax rotation, which maximizes the variance of the loadings of variables within factors. The highest loading of an indicator, then, defines to what factor it should be assigned.

**Pilot Test for Factor Analysis**

The pilot test is performed to test distribution of the variables - in this case the questions - on factors. For this research, the unit of measure is the organization. Therefore, it was required to have direct feedback from IT professionals working on IT security in each one of the organizations because they are the most qualified witnesses of the DFR status of their firms. In addition, they are the ones who better understand the technical terminology used in the questions. Because the surveys were directed to this specific respondent profile, many surveyed were discarded for not complying with the requirements. 20 out of 151 respondents who took the survey qualified as valid surveyed. The demographics of these respondents in terms of number of respondents per level in each question are shown below:

Table 11. Respondents' demographics from pilot study (Age)

| **Respondent's age** | |
|---|---|
| Below 18 | 0 |
| 18 to 25 | 2 |
| 26 to 40 | 10 |
| 41 to 60 | 8 |
| Above 60 | 0 |

Table 12. Respondents' demographics from pilot study (Gender)

| **Respondent's gender** | |
|---|---|
| Male | 14 |
| Female | 6 |

Table 13. Respondents' demographics from pilot study (Tenure)

| **Respondent's years in the organization** | |
|---|---|
| Less than 2 | 0 |
| 2 to 5 | 4 |
| 6 to 10 | 10 |
| 11 to 20 | 6 |
| More than 20 | 0 |

Table 14. Respondents’ demographics from pilot study (Position)

| Respondent's current position | |
|---|---|
| IT Director | 8 |
| It Analyst | 1 |
| CIO | 2 |
| CEO | 1 |
| Co Op | 1 |
| Superv. | 1 |
| CISO | 1 |
| Systems Architect | 1 |
| IT VP | 3 |
| Mngr | 1 |

Table 15. Respondents’ demographics from pilot study (Years in position)

| Respondent's years in position | |
|---|---|
| Less than 2 | 1 |
| 2 to 5 | 9 |
| 6 to 10 | 8 |
| 11 to 20 | 2 |
| More than 20 | 0 |

Each IT professional provides information about a specific organization. The demographics of these organizations in terms of number of organizations per level in each question are as follows:

Table 16. Organizations' demographics from pilot study (Industry)

| Organization's Industry | |
|---|---|
| Manufacturing and Process Industries (Non-computer) | 0 |
| Online Retailer | 1 |
| Internet Service Provider (ISP) or Application Service Provider (ASP) | 0 |
| Communications Carrier | 0 |
| Aerospace | 0 |
| Banking/Finance/Accounting | 3 |
| Insurance/Real Estate/Legal | 0 |
| Federal Government (including military) | 0 |
| State/Local Government | 1 |
| Medical/Dental/Healthcare | 3 |
| Transportation/Utilities | 1 |
| Construction/Architecture/Engineering | 1 |
| Data Processing Services | 1 |
| Wholesale/Retail/Distribution | 1 |
| Education | 4 |
| Marketing/Advertising/Entertainment | 0 |
| Research/Development Lab | 0 |
| Business Services/Consultant | 0 |
| Computer Manufacturer (Hardware, software, peripherals) | 0 |
| Computer/Network Services/Consultant | 4 |
| Computer Related Retailer/Wholesaler/Distributor | 0 |
| Other | 0 |

Table 17. Organizations' demographics from pilot study (Sales)

| Organization's Year Sales in $1000 | |
|---|---|
| Less than 50 | 0 |
| Between 50 and 200 | 0 |
| Between 200 and 500 | 1 |
| Between 500 and 2,000 | 7 |
| More than 2,000 | 12 |

Table 18. Organizations' demographics from pilot study (Employees)

| Organization's Number of Employees | |
|---|---|
| 1 to 50 | 0 |
| Between 51 and 200 | 3 |
| Between 201 and 500 | 6 |
| Between 501 and 2000 | 6 |
| More than 5,000 | 5 |

Table 19. Organizations' demographics from pilot study (Customers)

| Organization's Number of Customers | |
|---|---|
| 1 to 20 | 0 |
| Between 21 and 200 | 1 |
| Between 201 and 1,000 | 4 |
| Between 1,001 and 10,000 | 11 |
| More than 10,000 | 4 |

Table 20. Organizations' demographics from pilot study (Data)

| Organization's Monthly Produced Data | |
|---|---|
| Less than 10 MB | 0 |
| Between 10 and 500 MB | 0 |
| Between 0.5 and 50 GB | 2 |
| Between 50 GB and 1 TB | 5 |
| More than 1 TB | 13 |

**Results of Pilot Study**

18 questions represent perceptual variables and are, therefore, included in the search for factors that reflect the DFR status. As shown in the rotated factor matrix delivered by SPSS, six factors were found as representative of these 18 variables. A gray background shows the highest loading of each variable.

Table 21. Perceptual factors extracted from EFA

**Rotated Factor Matrix**[a]

| | Factor | | | | | |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 |
| Per1 | -0.461 | 0.024 | -0.276 | 0.118 | -0.556 | 0.036 |
| Per2 | 0.87 | -0.269 | 0.006 | -0.004 | 0.108 | 0.152 |
| Per3 | -0.261 | 0.731 | -0.181 | 0 | 0.269 | 0.022 |
| Per4 | -0.225 | 0.677 | 0 | -0.063 | 0.117 | 0.031 |
| Per5 | -0.014 | 0.238 | -0.062 | 0.079 | 0.965 | 0.015 |
| Per6 | -0.067 | 0.433 | -0.33 | -0.437 | 0.04 | 0.158 |
| Per7 | 0.278 | -0.231 | 0.22 | 0.043 | -0.027 | 0.904 |
| Per8 | 0.799 | -0.231 | 0.27 | 0.126 | 0.141 | 0.102 |
| Per9 | 0.354 | -0.288 | 0.457 | 0.148 | 0.202 | -0.009 |
| Per10 | 0.701 | -0.133 | -0.013 | 0.431 | -0.061 | -0.149 |
| Per11 | -0.182 | 0.927 | -0.09 | -0.173 | -0.112 | -0.238 |
| Per12 | 0.821 | -0.225 | 0.282 | -0.219 | -0.028 | 0.128 |
| Per13 | 0.07 | 0.085 | 0.72 | 0.163 | -0.112 | 0.335 |
| Per14 | -0.026 | -0.097 | 0.058 | 0.991 | 0.042 | 0.038 |
| Per15 | 0.528 | -0.194 | 0.444 | 0.325 | 0.263 | -0.085 |
| Per16 | 0.426 | -0.298 | 0.204 | 0.306 | -0.067 | -0.541 |
| Per17 | 0.476 | -0.347 | 0.768 | -0.084 | 0.146 | -0.134 |
| Per18 | -0.712 | 0.162 | -0.507 | 0.09 | 0.027 | 0.019 |

Extraction Method: Maximum Likelihood.

Rotation Method: Varimax with Kaiser Normalization.

a. Rotation converged in 10 iterations.

Factor analysis shows that six perceptual factors extracted explain 77% of the total variance explained by the set of 18 perceptual variables. The name of each factor was chosen based on the variable that has the highest loading on it, while making it general enough to account for all other variables in the factor. The following is a list of the factors with their corresponding variables and loadings, as well as the percentage of the variance of all variables that the factor explains. The questions are added as they show up in the questionnaire, but it should be remembered that they are introduced as something that the organization has, does, knows or is perceived, thus the reader should add those words accordingly.

Table 22. Perceptual variables per factor from pilot study

**Perceptual Factor 2: Hesitation**
**Variance 15%**

| Var | Load | Question |
|---|---|---|
| Per11 | 0.927 | Fulfilling the demands that the legal system makes about admissibility and reliability of digital evidence for our organization is hard. |
| Per3 | 0.731 | Implementing a digital forensics program is expensive. |
| Per4 | 0.677 | This organization is exposed to many risks and threats. |

**Perceptual Factor 3: Awareness**
**Variance 12.5%**

| Var | Load | Question |
|---|---|---|
| Per17 | 0.768 | How to forecast and control the escalation of costs when facing a digital forensic incident. |
| Per13 | 0.72 | A corporate culture of secrecy (forensics activities are kept from users) |
| Per9 | 0.457 | The organization's employees have knowledge of information management and security policies. |

**Perceptual Factor 4: Knowledge**
**Variance 9.7%**

| Var | Load | Question |
|---|---|---|
| Per14 | 0.991 | Whether or not to turn off a hacked system or device in case of a cyber incident. |
| Per6 | -0.44 | The location(s) of the organization makes it insecure. |

**Perceptual Factor 5: Self-image**
**Variance 8.5%**

| Var | Load | Question |
|---|---|---|
| Per5 | 0.965 | Our firm has a public profile. |
| Per1 | -0.56 | Given the definition of digital forensic readiness (DFR) as the state of preparedness to obtain, understand, and present verifiable digital evidence when needed, I would rate my organization's DFR as: |

**Perceptual Factor 6: Confidence**
**Variance 7.8%**

| Var | Load | Question |
|---|---|---|
| Per7 | 0.904 | The organization's policies on information systems monitoring are consistent with its personnel privacy policies and applicable employment law. |
| Per16 | -0.54 | How to anticipate the organization's discovery needs and accelerate its investigation in case of a cyber incident. |

53 questions were considered extant variables and therefore included in the search for factors that form the DFR status. As shown in the rotated factor matrix delivered by SPSS, 11 factors were found as representative of these 53 variables.

Table 23. Extant factors extracted from PCA

**Rotated Component Matrix**[a]

| | Component | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
| Ext1 | 0.229 | 0.646 | 0.27 | 0.184 | 0.395 | 0.115 | 0.083 | -0.005 | -0.22 | 0.006 | 0.38 |
| Ext2 | -0.005 | 0.167 | 0.139 | 0.159 | 0.2 | 0.07 | 0.011 | -0.029 | 0.914 | 0.057 | 0.008 |
| Ext3 | 0.091 | -0.103 | -0.117 | -0.075 | 0.084 | -0.034 | 0.933 | 0.11 | -0.1 | 0.117 | -0.073 |
| Ext4 | 0.452 | 0.576 | 0.154 | 0.2 | 0.373 | -0.003 | 0.142 | 0.38 | 0.168 | 0.093 | -0.037 |
| Ext5 | 0.583 | 0.626 | -0.123 | 0.158 | 0.215 | 0.207 | 0.158 | 0.043 | 0.269 | 0.019 | -0.034 |
| Ext6 | -0.014 | 0.651 | 0.358 | 0.063 | 0.193 | 0.441 | 0.138 | 0.258 | 0.202 | 0.123 | 0.085 |
| Ext7 | 0.182 | 0.873 | 0.205 | 0.02 | 0.268 | 0.014 | 0.128 | 0.075 | 0.019 | -0.059 | -0.07 |
| Ext8 | 0.198 | 0.673 | 0.196 | 0.192 | 0.054 | 0.522 | 0.137 | -0.074 | 0.278 | -0.047 | 0.04 |
| Ext9 | 0.524 | 0.265 | 0.074 | 0.637 | 0.063 | 0.132 | 0.11 | 0.002 | 0.259 | 0.02 | -0.307 |
| Ext10 | 0.363 | 0.704 | 0.097 | 0.32 | 0.032 | 0.086 | -0.258 | 0.144 | -0.091 | 0.076 | -0.077 |
| Ext11 | 0.029 | 0.04 | 0.235 | 0.262 | -0.039 | 0.25 | 0.856 | -0.121 | 0.021 | -0.004 | -0.002 |
| Ext12 | 0.287 | 0.322 | -0.033 | 0.809 | 0.184 | 0.191 | -0.024 | 0.026 | -0.007 | 0.109 | 0.143 |
| Ext13 | 0.239 | 0.308 | 0.079 | -0.053 | 0.583 | 0.441 | 0.026 | 0.432 | 0.129 | -0.213 | 0.048 |
| Ext14 | 0.326 | 0.255 | 0.167 | 0.085 | 0.716 | 0.145 | 0.148 | -0.014 | 0.294 | -0.244 | -0.156 |
| Ext15 | 0.024 | 0.082 | 0.39 | 0.805 | 0.12 | 0.25 | 0.083 | 0.172 | 0.188 | -0.093 | 0.071 |
| Ext16 | 0.722 | 0.088 | 0.177 | 0.4 | 0.217 | 0.192 | -0.09 | 0.039 | 0.072 | 0.116 | -0.335 |
| Ext17 | 0.51 | 0.479 | 0.191 | 0.401 | 0.005 | 0.06 | 0.105 | -0.179 | 0.371 | 0.031 | -0.319 |
| Ext18 | 0.228 | 0.249 | 0.264 | 0.384 | 0.1 | 0.776 | 0.107 | 0.068 | -0.092 | -0.041 | 0.015 |
| Ext19 | 0.791 | 0.313 | 0.179 | -0.016 | 0.294 | 0.034 | 0.073 | 0.048 | 0.057 | -0.247 | 0.058 |
| Ext20 | 0.703 | 0.386 | -0.107 | 0.134 | 0.43 | 0.028 | 0.086 | 0.235 | 0.099 | -0.069 | 0.133 |
| Ext21 | 0.173 | 0.16 | 0.818 | 0.184 | 0.233 | 0.103 | 0.136 | 0.262 | 0.206 | 0.059 | 0.028 |
| Ext22 | 0.313 | 0.604 | -0.148 | 0.206 | 0.214 | 0.545 | 0.138 | 0.199 | 0.211 | -0.024 | -0.093 |
| Ext23 | 0.221 | 0.094 | 0.083 | 0.075 | 0.936 | -0.025 | -0.009 | 0.005 | -0.007 | 0.062 | 0.011 |
| Ext24 | 0.199 | 0.177 | 0.624 | 0.272 | 0.192 | 0.523 | 0.111 | -0.25 | 0.038 | -0.144 | -0.056 |
| Ext25 | 0.766 | -0.106 | 0.271 | 0.283 | 0.089 | 0.222 | 0 | -0.009 | 0.047 | -0.099 | 0.361 |
| Ext26 | 0.104 | 0.231 | 0.009 | 0.105 | 0.063 | -0.044 | 0.884 | -0.046 | 0.171 | -0.094 | 0.072 |
| Ext27 | 0.44 | 0.103 | 0.612 | 0.378 | 0.128 | -0.081 | 0.144 | 0.022 | 0.125 | 0.011 | 0.441 |
| Ext28 | 0.592 | 0.044 | 0.176 | 0.388 | 0.162 | 0.347 | 0.015 | -0.018 | -0.046 | 0.452 | 0.026 |
| Ext29 | -0.028 | 0.455 | 0.46 | 0.276 | 0.13 | 0.102 | 0.001 | 0.031 | 0.072 | 0.132 | 0.156 |
| Ext30 | -0.048 | 0.202 | 0.203 | -0.245 | 0.017 | 0.092 | 0.689 | 0.533 | -0.08 | -0.019 | 0.078 |
| Ext31 | 0.672 | 0.228 | -0.126 | 0.18 | 0.179 | 0.112 | -0.056 | 0.59 | -0.011 | 0.118 | 0.143 |
| Ext32 | 0.288 | 0.076 | 0.606 | 0.052 | 0.002 | 0.67 | 0.011 | 0.153 | 0.096 | 0.067 | 0.087 |
| Ext33 | 0.388 | 0.454 | 0.336 | 0.071 | -0.043 | 0.474 | 0.014 | 0.102 | 0.129 | 0.479 | -0.114 |
| Ext34 | 0.09 | 0.078 | 0.69 | 0.263 | 0.292 | 0.085 | 0.008 | 0.053 | 0.322 | 0.019 | -0.351 |
| Ext35 | 0.117 | 0.272 | 0.097 | 0.372 | 0.725 | 0.107 | -0.017 | 0.002 | 0.117 | 0.222 | 0.111 |
| Ext36 | 0.382 | 0.466 | 0.2 | 0.538 | 0.23 | 0.044 | 0.182 | 0.331 | 0.122 | -0.066 | -0.062 |
| Ext37 | 0.3 | 0.245 | 0.414 | 0.341 | -0.128 | 0.108 | 0.109 | 0.643 | -0.139 | -0.085 | -0.043 |
| Ext38 | 0.325 | 0.186 | 0.828 | -0.131 | 0.005 | 0.214 | -0.028 | -0.013 | -0.175 | -0.057 | 0.051 |
| Ext39 | 0.628 | 0.511 | 0.12 | 0.108 | 0.074 | -0.134 | 0.001 | -0.039 | 0.129 | 0.455 | -0.013 |
| Ext40 | 0.83 | 0.15 | 0.167 | 0.407 | 0.001 | 0.11 | 0.07 | 0.032 | 0.076 | 0.036 | 0.207 |
| Ext41 | 0.021 | 0.564 | 0.096 | -0.056 | 0.534 | 0.2 | 0.254 | 0.133 | 0.086 | -0.297 | 0.056 |
| Ext42 | 0.722 | 0.263 | 0.309 | -0.19 | 0.329 | -0.079 | 0.105 | -0.277 | 0.049 | -0.039 | 0.071 |
| Ext43 | 0.43 | 0.2 | 0.534 | 0.397 | 0.097 | 0.084 | 0.063 | 0.017 | -0.134 | 0.378 | 0.192 |
| Ext44 | 0.83 | 0.143 | 0.369 | 0.125 | 0.108 | -0.012 | 0.033 | 0.155 | -0.1 | 0.076 | -0.205 |
| Ext45 | 0.842 | -0.024 | 0.241 | 0.012 | 0.288 | 0.076 | 0.029 | -0.062 | -0.128 | -0.031 | -0.183 |
| Ext46 | 0.43 | 0.401 | 0.179 | 0.071 | 0.295 | 0.292 | -0.068 | 0.072 | -0.238 | -0.54 | -0.067 |
| Ext47 | 0.611 | 0.355 | 0.394 | 0.236 | -0.033 | 0.202 | 0.273 | -0.008 | 0.215 | -0.108 | -0.195 |
| Ext48 | 0.284 | -0.012 | 0.359 | 0.585 | 0.475 | -0.019 | 0.029 | -0.103 | 0.108 | 0.155 | -0.21 |

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Ext49 | 0.215 | 0.411 | 0.369 | 0.27 | 0.53 | -0.041 | 0.004 | -0.099 | 0.003 | -0.131 | -0.005 |
| Ext50 | 0.847 | 0.076 | 0.133 | 0.202 | 0.068 | 0.367 | 0.117 | -0.03 | -0.023 | 0.121 | 0.134 |
| Ext51 | 0.779 | 0.225 | 0.114 | 0.352 | 0.217 | -0.135 | 0.093 | 0.22 | -0.107 | -0.069 | -0.02 |
| Ext52 | 0.696 | 0.034 | 0.199 | -0.024 | 0.014 | 0.29 | 0.048 | 0.274 | 0.051 | 0.191 | 0.489 |
| Ext53 | 0.764 | 0.282 | -0.179 | -0.144 | -0.079 | 0.257 | -0.106 | 0.197 | 0.089 | 0 | -0.085 |

Extraction Method: Principal Component Analysis.
Rotation Method: Varimax with Kaiser Normalization.
a Rotation converged in 12 iterations.

Although SPSS delivers 11 principal components or extant factors, no variable has its highest loading on factor 11. Moreover, no variable loaded above 0.5 in that factor. Therefore, only 10 extant factors are considered, which together explain around 90% of the total variance explained by the set of 53 extant variables:

Table 24. Extant variables per factor from pilot study

**Extant Factor 1: Preparedness**
**Variance 22.6%**

| Var | Load | Question |
|---|---|---|
| Ext50 | 0.847 | How to determine the nature, crime category, types of technologies used or involved, and technical skill and knowledge of a suspect in a cyber incident. |
| Ext45 | 0.842 | Which forensic tools and techniques the organization needs to deploy in case of a cyber incident. |
| Ext40 | 0.83 | Mature and adequate governance models as well as an information systems development life cycle (ISDLC) informed by a well-developed forensic readiness policy. |
| Ext44 | 0.83 | How to conduct an onsite examination keeping the integrity of the original evidence |
| Ext19 | 0.791 | Performs security benchmarking to assess the preparedness of competitors and enemies. |
| Ext51 | 0.779 | How to provide detailed log and documentation of the chain of evidence at every step, including information about the tools used, in case of a cyber incident. |
| Ext25 | 0.766 | A documented system security architecture configuration with consistent standards throughout the entire platform. |
| Ext53 | 0.764 | How to demonstrate due diligence and compliance with the organization's policies and all applicable laws and regulations in all phases of a forensic investigation process. |
| Ext16 | 0.722 | Develops corporate policies and procedures collaboratively using collaboration tools to maintain a shared workspace. |
| Ext42 | 0.722 | Multiple virtual locations, wired and wireless networks, and/or a mobile platform. |
| Ext20 | 0.703 | Policies clarifying ownership of data in corporate and personnel devices, use of systems, privacy, and consent of monitoring. |
| Ext52 | 0.696 | What the sources and format of the organization's data are, when and where data is generated, the associated threats to the data, and how data is preserved for long-term storage. |
| Ext31 | 0.672 | Archive management procedures to assure that records (including those in the cloud) possess content, context and structure, while preserving evidence quality in terms of authenticity, reliability, integrity, and usability. |
| Ext39 | 0.628 | A business continuity plan to minimize interruption to the business while gathering admissible evidence, to restore essential services during an attack, to avoid financial loss, and to recover assets and data. |
| Ext47 | 0.611 | How to determine whether a warrant allows for an onsite or in situ examination, seizure and removal of the system(s), in case of a cyber incident. |
| Ext28 | 0.592 | A proper laboratory, equipment, hardware and software for onsite computer forensic examiners. |
| Ext17 | 0.51 | Controls security information through dashboards and metrics that continuously and dynamically measure information security performance. |

**Extant Factor 2: Control**
**Variance 13.1%**

| Var | Load | Question |
|---|---|---|
| Ext7 | 0.873 | Identifies and prioritizes the sources of evidence, preserves logs and data, and assesses the value of potential evidence. |
| Ext10 | 0.704 | Controls access to data and evidence through strong authentication, access control lists, user logging, encryption, and implements measures for handling inadvertent exposures. |

|  |  |  |
|---|---|---|
| Ext8 | 0.673 | Controls information flow and channels to prevent anonymous activities and anti-forensic activities (e.g. password crackers, key-loggers, and steganography software) and assesses Internet activities such as cookies, temporary files, URLs, email, instant messages and SMTP send-receiver pairs. |
| Ext6 | 0.651 | Uses digital forensics tools and techniques, e.g., intrusion detection systems (IDS), security event management software (SEM), forensic kits, antivirus and spyware |
| Ext1 | 0.646 | The organization's security system has been proven to be reliable. |
| Ext5 | 0.626 | Offers and encourages personnel training and guidance in secure conduct and digital forensics tools and techniques. |
| Ext22 | 0.604 | Policies clarifying the roles and tasks to comply with statutory and/or governmental regulations (e.g. Sarbanes–Oxley, HIPAA, admissibility rules, reporting requirements, international law, and penalties for security incidents). |
| Ext4 | 0.576 | Enforces forensic policies and makes staff accountable of their digital forensic responsibilities and the use of digital forensic tools. |
| Ext41 | 0.564 | Storage technology that is appropriate in capacity and functionality, including storage visualization abilities. |

**Extant Factor 3: Policing**

**Variance 10.7%**

| Var | Load | Question |
|---|---|---|
| Ext38 | 0.828 | Sufficient decryption capabilities to counter the increasingly pervasive use of encryption technologies. |
| Ext21 | 0.818 | Policies defining potential incidents and how to respond to them. |
| Ext34 | 0.69 | Procedures for performing backups, gathering permanent and volatile data, and analyzing admissible evidence. |
| Ext24 | 0.624 | A quality assurance system, with good records, that covers policies, activities, procedures, training, roles, documentation, and management. |
| Ext27 | 0.612 | A change management database that includes file hashes for common operating system files and for deployed applications, using file integrity checking software on important assets. |
| Ext43 | 0.534 | Enough funding for the implementation of digital forensic readiness. |
| Ext29 | 0.46 | A secure storage of systems and networks activity logs with the associated meta-data identifying times and authors. |

**Extant Factor 4: Prevention**

**Variance 9.3%**

| Var | Load | Question |
|---|---|---|
| Ext12 | 0.809 | Looks for legal and technical advice, including published standards, regarding forensic policies, procedures, and information security, and monitors emerging academic digital forensics research. |
| Ext15 | 0.805 | Controls physical access to, classifies, and relocates corporate physical and digital assets according to a digital forensic program. |
| Ext9 | 0.637 | Develops the digital and physical infrastructure with forensic capabilities such as authentication traffic monitoring, tamper proof mechanisms and logging time synchronization. |
| Ext48 | 0.585 | How to recognize the range of personnel within the firm who may be involved in a legal inquiry, in case of a cyber incident. |
| Ext36 | 0.538 | The technology, expertise, and resources to perform computer and network forensics and manage legal evidence properly. |

**Extant Factor 5: Documentation**

**Variance 8.9%**

| Var | Load | Question |
|---|---|---|

| | | |
|---|---|---|
| Ext23 | 0.936 | A documented digital forensics investigation protocol describing roles and procedures to capture, store, map, analyze, preserve, control access to, integrate, and present evidence. |
| Ext35 | 0.725 | A process for the selection, use, testing, and maintenance of technology deployed in the organization's information systems and the forensic readiness program. |
| Ext14 | 0.716 | Profiles and monitors systems' users and their personal devices. |
| Ext13 | 0.583 | Conducts regular risk assessments and compliance reviews. |
| Ext49 | 0.53 | How to determine the location, remote access methods, time, timeline of events, and duration of a cyber incident. |

**Extant Factor 6: Investigation**

**Variance 6.9%**

| Var | Load | Question |
|---|---|---|
| Ext18 | 0.776 | Manages external digital forensic investigators, establishes their capabilities and response times, and validates the accreditation of their laboratories. |
| Ext32 | 0.67 | Procedures describing the configuration and use of active monitoring and logging mechanisms, including procedures to prevent alteration of intercepted communications. |

**Extant Factor 7: Permissiveness**

**Variance 6.5%**

| Var | Load | Question |
|---|---|---|
| Ext3 | 0.933 | Allows wireless access. |
| Ext26 | 0.884 | Archived reports of previous incidents, anomalous observations, crime and dispute history and lessons learned. |
| Ext11 | 0.856 | Bans disk scrubbing tools, file shredding software, personal file encryption, and anti-forensic strategies (e.g. anonymity, data destruction/alteration, and onion routing). |
| Ext30 | 0.689 | A suspicion policy to review potential sources of attacks or failure, complaints, crimes and disputes, and threats from opportunists, competitors or disgruntled employees. This policy indicates how to manage people leaving the company. |

**Extant Factor 8: Focus**

**Variance 4.3%**

| Var | Load | Question |
|---|---|---|
| Ext37 | 0.643 | Dedicated roles relating to security and forensics including first responders and investigators ready to work collaboratively with legal, IT, law enforcement, business, and auditing representatives in case of a cyber incident. |

**Extant Factor 9: Redress**

**Variance 3.9%**

| Var | Load | Question |
|---|---|---|
| Ext2 | 0.914 | Seeks accountability for intruders. |

**Extant Factor 10: Traceability**

**Variance 3.2%**

| Var | Load | Question |
|---|---|---|
| Ext46 | -0.54 | Where to look in the system to identify case specific evidence in case of a cyber incident. |
| Ext33 | 0.479 | Information security audit procedures that include protection of IT and business systems, and monitoring of the forensics process. |

### Summary of Pilot Study

The pilot study is done to assess the feasibility of the surveys and to have a first view of the content validity of the factors. However, conclusions about final factors are done over the final sample.

The number of factors extracted from the pilot was limited to those with Eigen values above or equal to one. The factor analysis delivers 16 factors, 6 perceptual factors and 10 extant factors. This is a very similar number to that of the dimensions found via Q-Sort test; 15 in that case. This hindsight is used in the definition of the number of factors to extract from the final sample, which is a key decision researchers make in the application of factor analysis.

The sample size is insufficient to make conclusive decisions. However, the pilot test shows that the survey, although long and in-depth, is feasible. Some respondents actually made comments such as "I loved this survey[,] very important," "great survey, would like to take more," "Nice survey!," and "Great survey, would complete another one like it." This improves the possibility that respondents will thoroughly complete the survey despite its length. It is also an indicator that questions were understood and informative. As expected, the results obtained in the pilot were suitable for exploratory factor analysis, in the perceptual set, and for principal components analysis in the extant set. The percentage of variance extracted for the perceptual and extant factors, 77% and 90% respectively, fall into acceptable levels for factor analysis in social sciences (Hair, Black, Bavin & Henderson 2010).

The refinement of factors could continue with the removal of variables and even reorganization of factors based on theoretical analysis. However, this should be done when the final survey is run and a more solid sample of observations is obtained. No variables are removed at this moment to avoid missing variance that could be explained by those variables or shared variance with other variables in the consolidation of factors. The names of factors from the pilot study are not final, but provide a glimpse for the denomination of final factors and the direction that the refinement of those factors can take.

### Final Study

A final survey was run among IT professionals using the same questionnaire tested under the pilot study. Unlike the pilot study's requirement of IT professionals working on the security area in IT departments, the final study relaxes this requirement and includes IT professionals working on IT departments. This decision acknowledges that all IT related personnel are nowadays inevitably involved in IT security. In addition, some managers and directors of IT departments, which make a considerable segment of potential respondents, could have skipped choosing security as one of their functions simply for not being involved in the traditionally technically-related tasks of firewall configurations, antivirus updates and backups. The final collection of responses confirms the appropriateness of this decision: IT managers, administrators, VPs, and CIOs are popular positions cited by respondents. 52% of those who finished the survey reported IT management as their role at work. The data was collected through Qualtrics between the months of March and April of 2017 among organizations in the U.S. 1.243 attempts to complete the survey were done. However, strict requirements for the time taken to complete the survey were implemented such that responses completed in less than 6 minutes were considered not acceptable. The average respondent took over 14 minutes and the median was over 10 minutes. Two control questions to verify that respondents were thoughtfully reading the questions were strategically added to the questionnaire. 250 respondents who comply with all the conditions and representing equal number of organizations were selected for the analysis. The complete demographics for the respondents and the organizations they represent are as follows:

Table 25. Respondents' demographics from final study (Age)

| **Respondent's age** | |
|---|---|
| Below 18 | 0 |
| 18 to 25 | 14 |
| 26 to 40 | 151 |
| 41 to 60 | 81 |
| Above 60 | 4 |

Table 26. Respondents' demographics from final study (Gender)

| **Respondent's gender** | |
|---|---|
| Male | 154 |
| Female | 96 |

Table 27. Respondents' demographics from final study (Tenure)

| Respondent's years in the organization | |
|---|---|
| Less than 2 | 25 |
| 2 to 5 | 84 |
| 6 to 10 | 85 |
| 11 to 20 | 44 |
| More than 20 | 12 |

Table 28. Respondents' demographics from final study (Years in position)

| Respondent's years in position | |
|---|---|
| Less than 2 | 44 |
| 2 to 5 | 142 |
| 6 to 10 | 41 |
| 11 to 20 | 21 |
| More than 20 | 2 |

Table 29. Organizations' demographics from final study (Industry)

| **Organization's Industry** | |
|---|---|
| Manufacturing and Process Industries (Non-computer) | 20 |
| Online Retailer | 3 |
| Internet Service Provider (ISP) or Application Service Provider (ASP) | 9 |
| Communications Carrier | 4 |
| Aerospace | 1 |
| Banking/Finance/Accounting | 9 |
| Insurance/Real Estate/Legal | 4 |
| Federal Government (including military) | 7 |
| State/Local Government | 6 |
| Medical/Dental/Healthcare | 23 |
| Transportation/Utilities | 6 |
| Construction/Architecture/Engineering | 1 |
| Data Processing Services | 11 |
| Wholesale/Retail/Distribution | 4 |
| Education | 10 |
| Marketing/Advertising/Entertainment | 3 |
| Research/Development Lab | 5 |
| Business Services/Consultant | 22 |
| Computer Manufacturer (Hardware, software, peripherals) | 31 |
| Computer/Network Services/Consultant | 50 |
| Computer Related Retailer/Wholesaler/Distributor | 8 |
| Other | 13 |

Table 30. Organizations' demographics from final study (Sales)

| **Organization's Year Sales in $1000** | |
|---|---|
| Less than 50 | 13 |
| Between 50 and 200 | 25 |
| Between 200 and 500 | 25 |
| Between 500 and 2,000 | 46 |
| More than 2,000 | 141 |

Table 31. Organizations' demographics from final study (Employees)

| **Organization's Number of Employees** | |
|---|---|
| 1 to 50 | 24 |
| Between 51 and 200 | 26 |
| Between 201 and 500 | 50 |
| Between 501 and 2000 | 68 |
| More than 5,000 | 82 |

Table 32. Organizations' demographics from final study (Customers)

| **Organization's Number of Customers** | |
|---|---|
| 1 to 20 | 7 |
| Between 21 and 200 | 35 |
| Between 201 and 1,000 | 49 |
| Between 1,001 and 10,000 | 64 |
| More than 10,000 | 95 |

Table 33. Organizations' demographics from final study (Data)

| **Organization's Monthly Data** | |
|---|---|
| Less than 10 MB | 3 |
| Between 10 and 500 MB | 13 |
| Between 0.5 and 50 GB | 41 |
| Between 50 GB and 1 TB | 72 |
| More than 1 TB | 121 |

The objectives of the EFA are twofold, data reduction for the extant variables and structure identification for the perceptual variables. In the case of the extant variables, this study assumes that they represent what DFR is, according to a comprehensive review of the literature. Even with the reduction of variables performed during this research the number of these variables, 53, is still large for a parsimonious model. Digital forensics experts will benefit from a statistically-based reduction of the variables into fewer factors. On the other hand, the 18 perceptual variables discovered may not tell the whole story about the reflective indicators of DFR. The literature reviewed is mostly of a practical nature rather than of a theoretical or concept-based nature; therefore, it is reasonable to assume that most of what DFR is made of has been contemplated, but perceptions of such DFR may remain to be covered.

Conceptual models of behavioral or perceptual indicators of DFR status have not been proposed by researchers; therefore, there are no grounds to suggest completeness of the perceptual factors found in the literature. Still, the perceptual factors inferred during the present review, while not comprehensive, can shed light on the underlying structure of the DFR latent perceptual factors. Consequently, structure identification is a better objective for the perceptual variables.

### Sample Size for Final Study

The sample size of the final study is 250 observations, roughly five times the number of the bigger of the two sets of variables (53 extant variables vs. 18 perceptual variables), which is recommended for EFA (Hair et al. 2010). The separation between extant and perceptual variables also avoids mixing dependent and independent variables in the analysis, as warned by Hair et al. Perceptual variables are a reflection of the real status of DFR represented by extant variables. Therefore, variables of both sets should not be mixed.

### Factorability of Data

Hair et al. (2010) recommend a visual exploration of the data to detect that sufficient correlation among variables and heterogeneity of those correlations exist in order to consider the data feasible for factor analysis. Correlations above 0.3 are considered appropriate. After visual exploration, both data sets provide evidence of their feasibility for factor analysis. Moreover, this research quantifies this evidence.

To do this, the number of substantial correlations was counted and their proportion in respect to the total correlations was calculated. The number of possible correlations among perceptual variables is 153, given by the formula n*(n-1)/2, where n = 18, the number of perceptual variables. Likewise, the number of possible correlations among extant variables is 1,378, where n = 53, the number of extant variables. As an example, the formula =IF(ABS(C3)>=0.3,1,0) in Excel, was used to assign a number one to the correlation in cell C3. The application of this formula with reference to the correlations' cells range identifies those correlations greater or equal to 0.3. The count was 69 for the perceptual correlations and 1,240 for the extant correlations, which corresponds to 45% and 90% of substantial correlations, respectively.

Partial correlations higher than 0.7 indicate that variables have high unique variance, leaving small variance that could be explained by other variables. This shows poor suitability for factor analysis according to Hair et al. (2010). A look at the anti-image matrices of both variable sets shows that no partial correlation was greater or equal to 0.7. Likewise, the Bartlett test of sphericity that reviews that there are significant correlations among the variables shows statistical significance with a p value that is inferior to 0.0005 for both perceptual and extant variables. These results indicate suitability for factor analysis.

The Kaiser-Meyer-Olkin measure of sampling adequacy (KMO MSA) is an indicator of the proportion of correlations over the sum of correlations and partial correlations. Kaiser proposes the following interpretation of the results: below 0.50, unacceptable; in the 0.50s, miserable; in the 0.60s, mediocre; in the 0.70s, middling; in the 0.80s, meritorious; and in the 0.90s, marvelous (Kaiser 1974). The KMO is 0.885 or “meritorious” for the perceptual set and 0.962 or “marvelous” for the extant set.

**Factor Extraction**

Initially, the latent root criterion is used for the extraction of factors from both sets of variables. This method extracts only factors accounting for the variance of at least one single variable, i.e. an Eigen value of one. An orthogonal Varimax rotation is applied to simplify the factor structure. The result of these extractions is four perceptual factors and eight extant components, as shown in the table below, where a dark gray background identifies the highest loading of each variable and the light gray background identifies significant loadings on other factors.

Table 34. Perceptual factors extracted through Latent Root Criterion (Eigen value = 1)

**Rotated Factor Matrix**[a]

| | Factor | | | |
|---|---|---|---|---|
| | 1 | 2 | 3 | 4 |
| Per7 | .696 | .142 | .002 | .017 |
| Per9 | .664 | .230 | .010 | .107 |
| Per8 | .613 | .394 | .106 | .190 |
| Per10 | .533 | .205 | .109 | .135 |
| Per14 | .504 | .132 | .080 | .292 |
| Per16 | .478 | .336 | .002 | .451 |
| Per15 | .474 | .081 | .188 | .402 |
| Per12 | .445 | .410 | .075 | .287 |
| Per1 | -.380 | -.808 | -.095 | -.092 |
| Per18 | -.519 | -.658 | -.027 | -.242 |
| Per2 | .485 | .553 | .101 | .186 |
| Per6 | -.005 | .006 | .677 | .116 |
| Per4 | .043 | .111 | .569 | .008 |
| Per11 | -.028 | -.028 | .546 | -.015 |
| Per3 | .089 | -.102 | .429 | .242 |
| Per13 | .051 | .247 | .388 | .067 |
| Per5 | .229 | .081 | .326 | .002 |
| Per17 | .278 | .309 | .214 | .700 |

Extraction Method: Maximum Likelihood.
Rotation Method: Varimax with Kaiser Normalization.[a]
a. Rotation converged in 7 iterations.

Table 35. Extant factors extracted through Latent Root Criterion (Eigen value = 1)

| Rotated Component Matrix[a] | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | Component | | | | | | | |
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| Ext6 | .692 | .171 | -.037 | .208 | .223 | .126 | .132 | .045 |
| Ext7 | .686 | .154 | .167 | .191 | .134 | .184 | .183 | .119 |
| Ext9 | .686 | .194 | .315 | .267 | .121 | .176 | .083 | .037 |
| Ext8 | .644 | .265 | .087 | .075 | .239 | .217 | .031 | .083 |
| Ext10 | .623 | .081 | .225 | -.051 | .330 | .183 | .139 | .095 |
| Ext1 | .572 | .214 | .257 | .274 | .157 | -.005 | .216 | -.041 |
| Ext12 | .550 | .180 | .245 | .317 | .166 | .349 | .104 | -.190 |
| Ext4 | .522 | .183 | .184 | .374 | .198 | .307 | .095 | -.102 |
| Ext13 | .481 | .169 | .174 | .168 | .236 | .460 | .178 | -.035 |
| Ext5 | .430 | .203 | .323 | .308 | .216 | .332 | .239 | -.062 |
| Ext52 | .088 | .740 | .009 | .011 | .218 | .011 | .226 | -.043 |
| Ext49 | .190 | .689 | .118 | .253 | .254 | .229 | .041 | .006 |
| Ext46 | .294 | .648 | .278 | .212 | -.050 | .160 | .200 | .121 |
| Ext48 | .066 | .620 | .197 | .266 | .196 | .239 | .040 | -.008 |
| Ext51 | .346 | .596 | .336 | .175 | .136 | .143 | .052 | .012 |
| Ext50 | .288 | .595 | .341 | .286 | .180 | .205 | .043 | .042 |
| Ext45 | .364 | .528 | .269 | .229 | .160 | .165 | .216 | .125 |
| Ext44 | .220 | .518 | .308 | .350 | .114 | .176 | .235 | -.083 |
| Ext53 | .333 | .463 | .404 | .070 | .312 | .157 | .130 | .020 |
| Ext35 | .401 | .247 | .588 | .105 | .249 | .182 | .085 | -.008 |
| Ext47 | .135 | .389 | .566 | .240 | .069 | .119 | .139 | .078 |
| Ext40 | .211 | .291 | .522 | .441 | .225 | .125 | .207 | -.023 |
| Ext27 | .056 | .225 | .520 | .421 | .179 | .271 | .195 | .180 |
| Ext31 | .276 | .185 | .482 | .381 | .363 | .201 | .065 | .049 |
| Ext38 | .191 | .306 | .467 | .331 | .216 | .248 | .101 | -.049 |
| Ext2 | .399 | .221 | .456 | .074 | .255 | .177 | .043 | -.100 |
| Ext26 | .245 | .251 | .451 | .396 | .255 | .219 | .168 | -.059 |
| Ext36 | .338 | .280 | .424 | .255 | .079 | .224 | .360 | -.113 |
| Ext39 | .110 | .343 | .407 | .197 | .371 | .256 | .217 | -.048 |
| Ext33 | .282 | .188 | .393 | .315 | .370 | .184 | .296 | .019 |
| Ext28 | .125 | .255 | .153 | .772 | .035 | .220 | .068 | .046 |
| Ext18 | .279 | .202 | .291 | .569 | .068 | .423 | -.077 | -.008 |
| Ext30 | .242 | .199 | .125 | .507 | .474 | .101 | .238 | .017 |
| Ext37 | .202 | .341 | .273 | .507 | .238 | .254 | .109 | .000 |
| Ext29 | .270 | .207 | .021 | .503 | .492 | .078 | .205 | .036 |
| Ext23 | .330 | .197 | .303 | .468 | .329 | .160 | -.027 | .071 |
| Ext17 | .290 | .130 | .278 | .424 | .287 | .363 | .143 | -.014 |
| Ext25 | .271 | .313 | .285 | .388 | .323 | -.040 | .257 | -.004 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Ext22 | .302 | .213 | .237 | .089 | .654 | .208 | .004 | -.035 |
| Ext20 | .335 | .234 | .050 | .096 | .623 | .098 | .170 | -.014 |
| Ext21 | .365 | .157 | .360 | .178 | .536 | .237 | .124 | -.039 |
| Ext32 | .132 | .145 | .429 | .250 | .509 | .252 | .187 | .086 |
| Ext24 | .234 | .219 | .296 | .323 | .506 | .166 | .092 | .124 |
| Ext16 | .374 | .193 | .240 | .080 | .379 | .341 | .288 | -.123 |
| Ext11 | .175 | .152 | .241 | .214 | .085 | .658 | .038 | .031 |
| Ext14 | .239 | .226 | -.001 | .258 | .187 | .623 | .142 | .027 |
| Ext15 | .284 | .171 | .268 | .071 | .168 | .584 | .153 | .034 |
| Ext19 | .274 | .143 | .411 | .346 | .216 | .506 | .135 | -.037 |
| Ext42 | .096 | .181 | -.106 | -.015 | .127 | .403 | .615 | .223 |
| Ext41 | .183 | .305 | .280 | .067 | .082 | .041 | .572 | -.086 |
| Ext34 | .325 | .109 | .210 | .169 | .355 | .064 | .539 | .028 |
| Ext43 | .177 | .108 | .256 | .453 | .126 | .094 | .525 | -.023 |
| Ext3 | .074 | .027 | .019 | .037 | .015 | .019 | .029 | .918 |

Extraction Method: Principal Component Analysis.
Rotation Method: Varimax with Kaiser Normalization.[a]
a. Rotation converged in 14 iterations.

Several considerations must be taken into account before settling for the factors extracted, such that conceptual bases and statistical support are maintained. First, the statistical significance of loadings should be evaluated under stricter levels than those of correlation coefficients, given the larger standard errors of loadings. In order to obtain a 0.05 significance level for a sample of 250 observations, a target power level of 80% is achieved with minimum factor loadings of 0.35 (Hair et al. 2010). Only the perceptual variable PER5 (Our firm has a public profile) loading on factor 3 has a factor loading below this limit, at 0.326. Given that PER5 also has a low communality of 0.165 (i.e., small variance that is explained by other perceptual variables) it becomes a candidate for deletion. This is shown with gray background in the table of communalities below. This does not mean that the perception in an organization of having a public profile is not a reflection of its DFR status, but simply that no other variable in the set of perceptual variables of this research explains a similar construct significantly. All other perceptual and extant variables have factor loadings above the significant level of 0.35.

Regarding communalities, nine other perceptual variables have what is considered low levels (below 0.5 or at least half of their variance explained by other variables in their respective set). All of the extant variables have communalities above 0.5. These values coincide with the assumption that the set of perceptual variables is unlikely to be as comprehensive as the set of extant variables given the technical orientation of the current literature in DFR. It is expected that future research can detect more perceptual variables of DFR sharing variance with those proposed here.

Table 36. Communalities on Four-factor Perceptual Solution

| **Communalities of Perceptual Variables** | | |
|---|---|---|
| | Initial | Extraction |
| Per1 | 0.672 | 0.815 |
| Per2 | 0.62 | 0.586 |
| Per3 | 0.218 | 0.261 |
| Per4 | 0.31 | 0.338 |
| Per5 | 0.197 | 0.165 |
| Per6 | 0.317 | 0.472 |
| Per7 | 0.396 | 0.504 |
| Per8 | 0.589 | 0.578 |
| Per9 | 0.46 | 0.505 |
| Per10 | 0.339 | 0.356 |
| Per11 | 0.259 | 0.3 |
| Per12 | 0.497 | 0.455 |
| Per13 | 0.252 | 0.218 |
| Per14 | 0.373 | 0.363 |
| Per15 | 0.405 | 0.428 |
| Per16 | 0.505 | 0.545 |
| Per17 | 0.495 | 0.708 |
| Per18 | 0.735 | 0.762 |
| Extraction Method: Maximum Likelihood. | | |

Table 37. Communalities on Eight-Factor Extant Solution

| Communalities of Extant Variables | | |
|---|---|---|
| | Initial | Extraction |
| Ext1 | 1 | 0.588 |
| Ext2 | 1 | 0.529 |
| Ext3 | 1 | 0.853 |
| Ext4 | 1 | 0.633 |
| Ext5 | 1 | 0.644 |
| Ext6 | 1 | 0.638 |
| Ext7 | 1 | 0.658 |
| Ext8 | 1 | 0.61 |
| Ext9 | 1 | 0.732 |
| Ext10 | 1 | 0.619 |
| Ext11 | 1 | 0.6 |
| Ext12 | 1 | 0.692 |
| Ext13 | 1 | 0.619 |
| Ext14 | 1 | 0.618 |
| Ext15 | 1 | 0.582 |
| Ext16 | 1 | 0.599 |
| Ext17 | 1 | 0.593 |
| Ext18 | 1 | 0.717 |
| Ext19 | 1 | 0.707 |
| Ext20 | 1 | 0.606 |
| Ext21 | 1 | 0.679 |
| Ext22 | 1 | 0.672 |
| Ext23 | 1 | 0.599 |
| Ext24 | 1 | 0.603 |
| Ext25 | 1 | 0.575 |
| Ext26 | 1 | 0.628 |
| Ext27 | 1 | 0.677 |
| Ext28 | 1 | 0.756 |
| Ext29 | 1 | 0.661 |
| Ext30 | 1 | 0.664 |
| Ext31 | 1 | 0.667 |
| Ext32 | 1 | 0.649 |
| Ext33 | 1 | 0.627 |
| Ext34 | 1 | 0.611 |
| Ext35 | 1 | 0.68 |
| Ext36 | 1 | 0.636 |
| Ext37 | 1 | 0.621 |
| Ext38 | 1 | 0.579 |
| Ext39 | 1 | 0.587 |

| | | |
|---|---|---|
| Ext40 | 1 | 0.706 |
| Ext41 | 1 | 0.552 |
| Ext42 | 1 | 0.66 |
| Ext43 | 1 | 0.615 |
| Ext44 | 1 | 0.639 |
| Ext45 | 1 | 0.651 |
| Ext46 | 1 | 0.711 |
| Ext47 | 1 | 0.592 |
| Ext48 | 1 | 0.595 |
| Ext49 | 1 | 0.708 |
| Ext50 | 1 | 0.713 |
| Ext51 | 1 | 0.661 |
| Ext52 | 1 | 0.656 |
| Ext53 | 1 | 0.633 |

Extraction Method: Principal Component Analysis.

On the other hand, 7 perceptual and 26 extant variables present more than one significant factor loading. These cross-loadings are:

Table 38. Cross-loadings

| Variables | Factors |
|---|---|
| PER8, PER16, PER1, PER18 and PER2 | Factors 1 and 2 |
| PER16 and PER15 | Factors 1 and 4 |
| EXT4 | Factors 1 and 4 |
| EXT13 | Factors 1 and 6 |
| EXT45 | Factors 1 and 2 |
| EXT44 | Factors 2 and 4 |
| EXT53 and EXT47 | Factors 2 and 3 |
| EXT35 and EXT2 | Factors 1 and 3 |
| EXT40, EXT27 and EXT26 | Factors 3 and 4 |
| EXT36 | Factors 3 and 7 |
| EXT31 | Factors 3, 4 and 5 |
| EXT39, EXT33 and EXT32 | Factors 3 and 5 |
| EXT18 and EXT17 | Factors 4 and 6 |
| EXT30 and EXT29 | Factors 4 and 5 |
| EXT21 | Factors 1, 3 and 5 |
| EXT16 | Factors 1 and 5 |
| EXT19 | Factors 3 and 6 |
| EXT42 | Factors 6 and 7 |
| EXT34 | Factors 5 and 7 |
| EXT43 | Factors 4 and 7 |

Different extraction criteria, rotation methods, and/or deletion of variables can improve significance of loadings and reduce cross-loadings.

Another consideration to explore about the loadings is regarding factors defined by a single variable, which make it impractical to assess reliability. This assessment aims to reduce measurement errors by testing that the items in a factor are consistently measuring the same construct. One variable in each set falls under this condition PER17 and EXT3. However, they both have high loadings on the factor they define and non-significant loading in others, which means that deleting them, could not only eliminate the variables, but also a potential real factor from the model. Assessment of reliability on those factors defined by a single variable is left for future research if/when new variables for those factors are found.

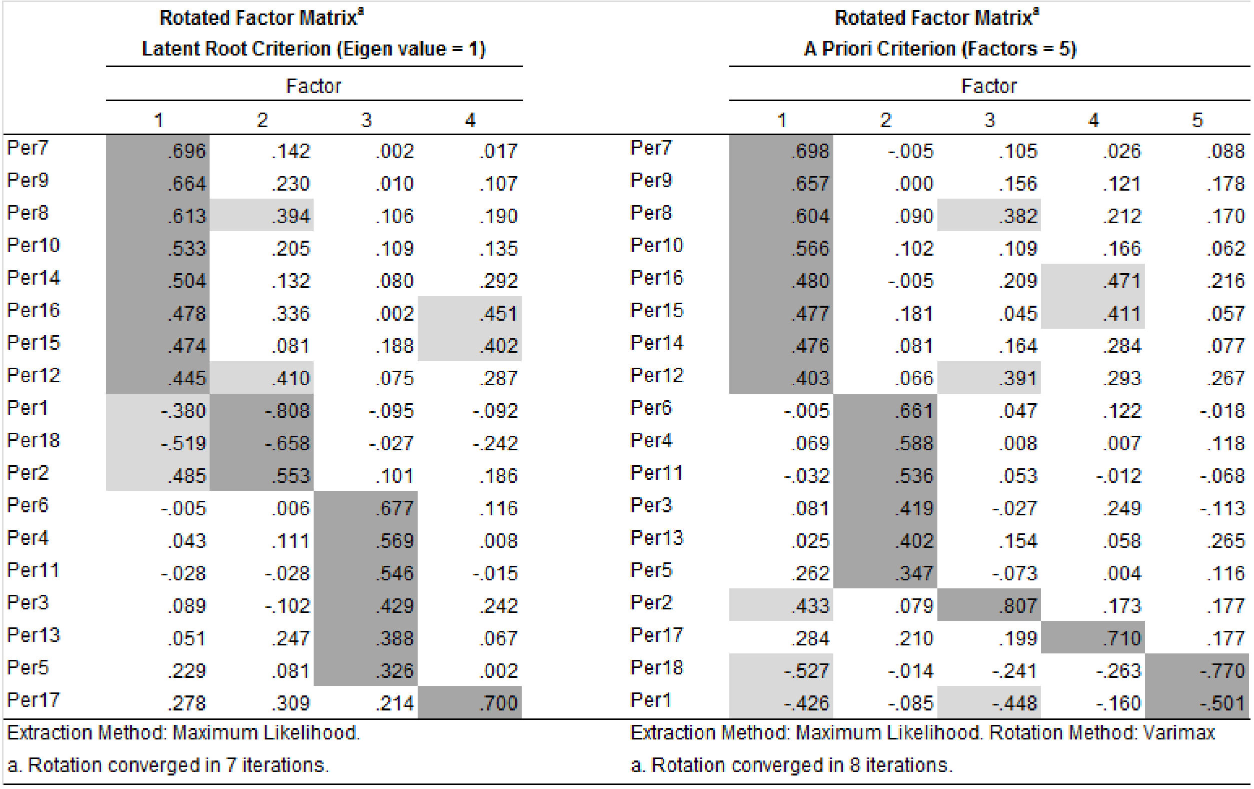
Finally, there is the evaluation of the variance extracted after rotation, which is 46.45% for perceptual factors and 64.33% for the extant ones. Hair et al. (2010) assert that a 60% or even lower level of total variance extracted is commonly accepted as satisfactory in the social sciences. Given that the variance explained by the extant factors is above 60% with all variable loadings being significant, analysis and labeling proceeds with the factors extracted. For the perceptual factors, extra refinement can increase the variance explained and the significance of PER5, as well as a better simplification of their structure.

Deletion of variables is avoided for different reasons in each set of variables. In the case of the extant variables, each of the variables tested is the product of thorough conceptual analysis of the extant literature and thus is deemed to have an important meaning for the definition of DFR. Those variables' cross-loadings over different factors might not be due to a problem of the variables but due to a problem in the definition of the factors. Therefore, eliminating variables will leave us with an incomplete view of DFR. The elimination of variables from the perceptual set, on the other hand, is not recommended for a different reason. It is clear in this research that the perceptual set that arose from the literature does not give a complete reflection of a DFR status. Thus, the lack of significance of a variable and the cross-loadings of others might not respond to poor variables, but to the absence of other variables that help shape the structure of the perceptual factors. Because this is an exploratory approach to a model of DFR, future researchers will benefit from testing all possible significant factors found in this research. Therefore, the refinement will aim to produce a factor model with as many as possible significant variables.

It should be noted that the factors extracted in the final study, four perceptual and eight extant, are fewer than those extracted in the pilot study and the dimensions of DFR for practitioners resulting from the Q-Sort test. In the case of the perceptual variables, this confirms Hair et al.'s contention that for fewer than 20 variables the latent root criterion extracts a conservative number of factors. Considering that the pilot study and the Q-Sort test are the only antecedents available for the application of an *a priori* criterion for the number of factors to extract, new factor analyses are run to extract more perceptual factors.

The comparison between the four-factor extraction obtained under the latent root criterion and a five-factor extraction with an *a priori* criterion are shown below. The same number of variables has cross-loadings, but PER1 has an additional cross-loading, thus, cross-loadings increase instead of decrease. A benefit of the five-factor extraction, though, is that PER5's factor loading of 0.326 increases to 0.347, very close to significance, but still below it. Likewise, its communality increases from 0.165 to 0.208 and the total variance explained increases from 46.45 to 49.4%.

Table 39. Comparison between four and five factor solutions



Rotated Factor Matrix[a]
Latent Root Criterion (Eigen value = 1)

| | Factor | | | |
|---|---|---|---|---|
| | 1 | 2 | 3 | 4 |
| Per7 | .696 | .142 | .002 | .017 |
| Per9 | .664 | .230 | .010 | .107 |
| Per8 | .613 | .394 | .106 | .190 |
| Per10 | .533 | .205 | .109 | .135 |
| Per14 | .504 | .132 | .080 | .292 |
| Per16 | .478 | .336 | .002 | .451 |
| Per15 | .474 | .081 | .188 | .402 |
| Per12 | .445 | .410 | .075 | .287 |
| Per1 | -.380 | -.808 | -.095 | -.092 |
| Per18 | -.519 | -.658 | -.027 | -.242 |
| Per2 | .485 | .553 | .101 | .186 |
| Per6 | -.005 | .006 | .677 | .116 |
| Per4 | .043 | .111 | .569 | .008 |
| Per11 | -.028 | -.028 | .546 | -.015 |
| Per3 | .089 | -.102 | .429 | .242 |
| Per13 | .051 | .247 | .388 | .067 |
| Per5 | .229 | .081 | .326 | .002 |
| Per17 | .278 | .309 | .214 | .700 |

Extraction Method: Maximum Likelihood.
a. Rotation converged in 7 iterations.

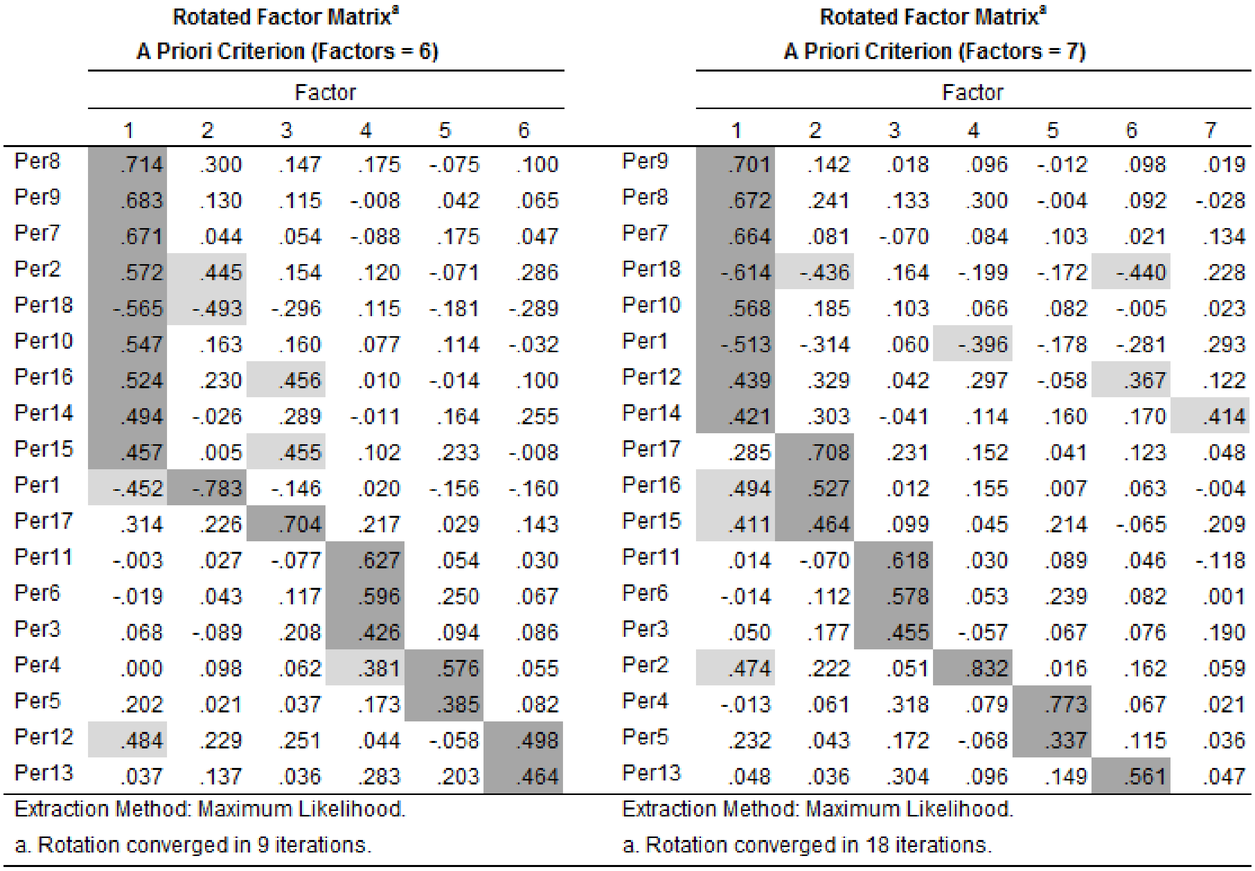
Rotated Factor Matrix[a]
A Priori Criterion (Factors = 5)

| | Factor | | | | |
|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 |
| Per7 | .698 | -.005 | .105 | .026 | .088 |
| Per9 | .657 | .000 | .156 | .121 | .178 |
| Per8 | .604 | .090 | .382 | .212 | .170 |
| Per10 | .566 | .102 | .109 | .166 | .062 |
| Per16 | .480 | -.005 | .209 | .471 | .216 |
| Per15 | .477 | .181 | .045 | .411 | .057 |
| Per14 | .476 | .081 | .164 | .284 | .077 |
| Per12 | .403 | .066 | .391 | .293 | .267 |
| Per6 | -.005 | .661 | .047 | .122 | -.018 |
| Per4 | .069 | .588 | .008 | .007 | .118 |
| Per11 | -.032 | .536 | .053 | -.012 | -.068 |
| Per3 | .081 | .419 | -.027 | .249 | -.113 |
| Per13 | .025 | .402 | .154 | .058 | .265 |
| Per5 | .262 | .347 | -.073 | .004 | .116 |
| Per2 | .433 | .079 | .807 | .173 | .177 |
| Per17 | .284 | .210 | .199 | .710 | .177 |
| Per18 | -.527 | -.014 | -.241 | -.263 | -.770 |
| Per1 | -.426 | -.085 | -.448 | -.160 | -.501 |

Extraction Method: Maximum Likelihood. Rotation Method: Varimax
a. Rotation converged in 8 iterations.

A six-factor extraction delivers the same number of cross-loadings than with the latent root criterion, but brings all variables to significance, while increasing the variance explained to 51.63%. An extraction of seven factors delivers similar results to those of the six-factor extraction, but no variable has its highest loading on the seventh factor.

Table 40. Comparison between six and seven factor solutions



**Rotated Factor Matrix[a]**
**A Priori Criterion (Factors = 6)**

| | Factor | | | | | |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 |
| Per8 | .714 | .300 | .147 | .175 | -.075 | .100 |
| Per9 | .683 | .130 | .115 | -.008 | .042 | .065 |
| Per7 | .671 | .044 | .054 | -.088 | .175 | .047 |
| Per2 | .572 | .445 | .154 | .120 | -.071 | .286 |
| Per18 | -.565 | -.493 | -.296 | .115 | -.181 | -.289 |
| Per10 | .547 | .163 | .160 | .077 | .114 | -.032 |
| Per16 | .524 | .230 | .456 | .010 | -.014 | .100 |
| Per14 | .494 | -.026 | .289 | -.011 | .164 | .255 |
| Per15 | .457 | .005 | .455 | .102 | .233 | -.008 |
| Per1 | -.452 | -.783 | -.146 | .020 | -.156 | -.160 |
| Per17 | .314 | .226 | .704 | .217 | .029 | .143 |
| Per11 | -.003 | .027 | -.077 | .627 | .054 | .030 |
| Per6 | -.019 | .043 | .117 | .596 | .250 | .067 |
| Per3 | .068 | -.089 | .208 | .426 | .094 | .086 |
| Per4 | .000 | .098 | .062 | .381 | .576 | .055 |
| Per5 | .202 | .021 | .037 | .173 | .385 | .082 |
| Per12 | .484 | .229 | .251 | .044 | -.058 | .498 |
| Per13 | .037 | .137 | .036 | .283 | .203 | .464 |

Extraction Method: Maximum Likelihood.
a. Rotation converged in 9 iterations.

**Rotated Factor Matrix[a]**
**A Priori Criterion (Factors = 7)**

| | Factor | | | | | | |
|---|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| Per9 | .701 | .142 | .018 | .096 | -.012 | .098 | .019 |
| Per8 | .672 | .241 | .133 | .300 | -.004 | .092 | -.028 |
| Per7 | .664 | .081 | -.070 | .084 | .103 | .021 | .134 |
| Per18 | -.614 | -.436 | .164 | -.199 | -.172 | -.440 | .228 |
| Per10 | .568 | .185 | .103 | .066 | .082 | -.005 | .023 |
| Per1 | -.513 | -.314 | .060 | -.396 | -.178 | -.281 | .293 |
| Per12 | .439 | .329 | .042 | .297 | -.058 | .367 | .122 |
| Per14 | .421 | .303 | -.041 | .114 | .160 | .170 | .414 |
| Per17 | .285 | .708 | .231 | .152 | .041 | .123 | .048 |
| Per16 | .494 | .527 | .012 | .155 | .007 | .063 | -.004 |
| Per15 | .411 | .464 | .099 | .045 | .214 | -.065 | .209 |
| Per11 | .014 | -.070 | .618 | .030 | .089 | .046 | -.118 |
| Per6 | -.014 | .112 | .578 | .053 | .239 | .082 | .001 |
| Per3 | .050 | .177 | .455 | -.057 | .067 | .076 | .190 |
| Per2 | .474 | .222 | .051 | .832 | .016 | .162 | .059 |
| Per4 | -.013 | .061 | .318 | .079 | .773 | .067 | .021 |
| Per5 | .232 | .043 | .172 | -.068 | .337 | .115 | .036 |
| Per13 | .048 | .036 | .304 | .096 | .149 | .561 | .047 |

Extraction Method: Maximum Likelihood.
a. Rotation converged in 18 iterations.

The same exercise of extracting more *a priori* factors for the extant set was run for 9, 10, 11, 12 and 13 factors, resulting in the eleven-factor model being the solution with fewer cross-loadings while keeping all variables significant. The thirteen-factor solution failed to converge after 25 iterations. It does deliver fewer cross-loadings after converging at the thirtieth iteration, but four of them become single-variable factors, in contrast to two in the ten and eleven-factor solutions. Still, the decision between the eleven-factor solution with fewer cross-loadings and the initially extracted eight-factor solution can be decided in favor of parsimony, following Hair et al.'s (2010) warning that for more than 50 variables, the latent root criteria tends to deliver too many factors. Thus, eight factors should be sufficient.

The labeling of factors proceeds, then, with the eight-factor solution of the extant set and the six-factor solution of the perceptual set, both presenting significant factor loadings for all variables. In these solutions, most cross-loadings appear in variables which are not those with the highest loading in a factor; hence, they will not affect labeling. The only exception is PER12, which is the main variable loading 0.498

in factor 6 and cross-loading 0.484 in factor 1. This cross-loading is considered in the labeling of perceptual factors 1 and 6.

### Reliability

Reliability is measured through Cronbach's Alpha. Two perceptual variables show negative loadings, PER1 and PER18, but the former defines a single-variable factor whereas the latter is part of factor one. Therefore, PER18 must be reverse scored in order to approprietaly calculate the Cronbach's Alpha for that factor. All extant factors have Cronbach's Alphas in the generally accepted level of 0.7, except for factor eight which Cronbach's Alpha cannot be calculated because it is a single-variable factor.

Likewise, two perceptual factors' Cronbach's Alpha cannot be calculated for the same reason. Perceptual factors 4, 5, and 6 have Cronbach's Alpha of 0.584, 0.489, and 0.423, respectively. Only factor one in the perceptual set has a Cronbach's Alpha above 0.7. It is expected that future research can discover additional perceptual factors with more satisfactory reliability measures.

### Factors from Final Study

The following is a list of the factors with their corresponding variables and loadings, as well as the percentage of the variance of all variables that the factor explains and the reliability measure of each factor. Appendix F (Final Survey) can be used o determine whether the item refers to something that the organization has, does, knows or perceives.

Table 41. Perceived Organizational Commitment (COMM)

| **Perceived Organizational Commitment** | | |
|---|---|---|
| **Cronbach's Alpha 0.855**<br>**Variance 20.5%** | | |
| **Var** | **Load** | **Question** |
| Per8 | .714 | The organization's personnel is committed to the forensics program and implement lessons learned from previous incidents. |
| Per9 | .683 | The organization's employees have knowledge of information management and security policies. |
| Per7 | .671 | The organization's policies on information systems monitoring are consistent with its personnel privacy policies and applicable employment law. |
| Per2 | .572 | Management is convinced of the importance of digital forensic readiness. |
| Per10 | .547 | Information technology and information security objectives are aligned with the business mission and objectives. |
| Per16 | .524 | How to anticipate the organization's discovery needs and accelerate its investigation in case of a cyber incident. |
| Per14 | .494 | Whether or not to turn off a hacked system or device in case of a cyber incident. |
| Per15 | .457 | How to handle a politically sensitive or publicly embarrassing incident. |

Table 42. Summary of DFR Assessment (SDFR)

| **Summary of DFR Assessment** | | |
|---|---|---|
| **Cronbach's Alpha 0.865**<br>**Variance 7.7%** | | |
| **Var** | **Load** | **Question** |
| Per1 | -.783 | Given the definition of digital forensic readiness (DFR) as the state of preparedness to obtain, understand, and present verifiable digital evidence when needed, I would rate my organization's DFR as: |
| Per18 | -.565 | After completing this survey and given the definition of digital forensic readiness (DFR) as the state of preparedness to obtain, understand, and present verifiable digital evidence when needed, I would rate my organization's DFR as: |

Table 43. Perceived Response Control (RESP)

| **Perceived Response Control** | | |
|---|---|---|
| **Cronbach's Alpha N/A**<br>**Variance 7.3%** | | |
| **Var** | **Load** | **Question** |
| Per17 | .704 | How to forecast and control the escalation of costs when facing a digital forensic incident. |

Table 44. Perceived Burden (BURD)

**Perceived Burden**

**Cronbach's Alpha 0.584**
**Variance 7.3%**

| Var | Load | Question |
|---|---|---|
| Per11 | .627 | Fulfilling the demands that the legal system makes about admissibility and reliability of digital evidence for our organization is hard. |
| Per6 | .596 | The location(s) of the organization makes it insecure. |
| Per3 | .426 | Implementing a digital forensics program is expensive. |

Table 45. Perceived Exposure (EXPO)

**Perceived Exposure**

**Cronbach's Alpha 0.489**
**Variance 4.4%**

| Var | Load | Question |
|---|---|---|
| Per4 | .576 | This organization is exposed to many risks and threats. |
| Per5 | .385 | Our firm has a public profile. |

Table 46. Perceived DFR Culture (CULT)

**Perceived DFR culture**

**Cronbach's Alpha 0.423**
**Variance 4.4%**

| Var | Load | Question |
|---|---|---|
| Per12 | .498 | A forensic culture of preserving evidence and sharing knowledge in computer security and digital forensics. |
| Per13 | .464 | A corporate culture of secrecy (forensics activities are kept from users) |

Table 47. Extant Technological Capacity (TECH)

| **Technological Capacity** | | |
|---|---|---|
| **Cronbach's Alpha 0.916**<br>**Variance 12.2%** | | |
| **Var** | **Load** | **Question** |
| Ext6 | .692 | Uses digital forensics tools and techniques, e.g., intrusion detection systems (IDS), security event management software (SEM), forensic kits, antivirus and spyware |
| Ext7 | .686 | Identifies and prioritizes the sources of evidence, preserves logs and data, and assesses the value of potential evidence. |
| Ext9 | .686 | Develops the digital and physical infrastructure with forensic capabilities such as authentication traffic monitoring, tamper proof mechanisms and logging time synchronization. |
| Ext8 | .644 | Controls information flow and channels to prevent anonymous activities and anti-forensic activities (e.g. password crackers, key-loggers, and steganography software) and assesses Internet activities such as cookies, temporary files, URLs, email, instant messages and SMTP send-receiver pairs. |
| Ext10 | .623 | Controls access to data and evidence through strong authentication, access control lists, user logging, encryption, and implements measures for handling inadvertent exposures. |
| Ext1 | .572 | The organization's security system has been proven to be reliable. |
| Ext12 | .550 | Looks for legal and technical advice, including published standards, regarding forensic policies, procedures, and information security, and monitors emerging academic digital forensics research. |
| Ext4 | .522 | Enforces forensic policies and makes staff accountable of their digital forensic responsibilities and the use of digital forensic tools. |
| Ext13 | .481 | Conducts regular risk assessments and compliance reviews. |
| Ext5 | .430 | Offers and encourages personnel training and guidance in secure conduct and digital forensics tools and techniques. |

Table 48. Extant Incident & Evidence Expertise (IEXP)

| **Incident & Evidence Expertise** | | |
|---|---|---|
| **Cronbach's Alpha 0.919**<br>**Variance 10.2%** | | |
| **Var** | **Load** | **Question** |
| Ext52 | .740 | What the sources and format of the organization's data are, when and where data is generated, the associated threats to the data, and how data is preserved for long-term storage. |
| Ext49 | .689 | How to determine the location, remote access methods, time, timeline of events, and duration of a cyber incident. |
| Ext46 | .648 | Where to look in the system to identify case specific evidence in case of a cyber incident. |
| Ext48 | .620 | How to recognize the range of personnel within the firm who may be involved in a legal inquiry, in case of a cyber incident. |
| Ext51 | .596 | How to provide detailed log and documentation of the chain of evidence at every step, including information about the tools used, in case of a cyber incident. |
| Ext50 | .595 | How to determine the nature, crime category, types of technologies used or involved, and technical skill and knowledge of a suspect in a cyber incident. |
| Ext45 | .528 | Which forensic tools and techniques the organization needs to deploy in case of a cyber incident. |
| Ext44 | .518 | How to conduct an onsite examination keeping the integrity of the original evidence |
| Ext53 | .463 | How to demonstrate due diligence and compliance with the organization's policies and all applicable laws and regulations in all phases of a forensic investigation process. |

Table 49. Extant DFR Embeddedness (EMBD)

**DFR Embeddedness**

**Cronbach's Alpha 0.928**
**Variance 9.8%**

| Var | Load | Question |
|---|---|---|
| Ext35 | .588 | A process for the selection, use, testing, and maintenance of technology deployed in the organization's information systems and the forensic readiness program. |
| Ext47 | .566 | How to determine whether a warrant allows for an onsite or in situ examination, seizure and removal of the system(s), in case of a cyber incident. |
| Ext40 | .522 | Mature and adequate governance models as well as an information systems development life cycle (ISDLC) informed by a well-developed forensic readiness policy. |
| Ext27 | .520 | A change management database that includes file hashes for common operating system files and for deployed applications, using file integrity checking software on important assets. |
| Ext31 | .482 | Archive management procedures to assure that records (including those in the cloud) possess content, context and structure, while preserving evidence quality in terms of authenticity, reliability, integrity, and usability. |
| Ext38 | .467 | Sufficient decryption capabilities to counter the increasingly pervasive use of encryption technologies. |
| Ext2 | .456 | Seeks accountability for intruders. |
| Ext26 | .451 | Archived reports of previous incidents, anomalous observations, crime and dispute history and lessons learned. |
| Ext36 | .424 | The technology, expertise, and resources to perform computer and network forensics and manage legal evidence properly. |
| Ext39 | .407 | A business continuity plan to minimize interruption to the business while gathering admissible evidence, to restore essential services during an attack, to avoid financial loss, and to recover assets and data. |
| Ext33 | .393 | Information security audit procedures that include protection of IT and business systems, and monitoring of the forensics process. |

Table 50. Extant Investigative Capacity (INVE)

| **Investigative Capacity** | | |
|---|---|---|
| **Cronbach's Alpha 0.897**<br>**Variance 9.6%** | | |
| **Var** | **Load** | **Question** |
| Ext28 | .772 | A proper laboratory, equipment, hardware and software for onsite computer forensic examiners. |
| Ext18 | .569 | Manages external digital forensic investigators, establishes their capabilities and response times, and validates the accreditation of their laboratories. |
| Ext30 | .507 | A suspicion policy to review potential sources of attacks or failure, complaints, crimes and disputes, and threats from opportunists, competitors or disgruntled employees. This policy indicates how to manage people leaving the company. |
| Ext37 | .507 | Dedicated roles relating to security and forensics including first responders and investigators ready to work collaboratively with legal, IT, law enforcement, business, and auditing representatives in case of a cyber incident. |
| Ext29 | .503 | A secure storage of systems and networks activity logs with the associated meta-data identifying times and authors. |
| Ext23 | .468 | A documented digital forensics investigation protocol describing roles and procedures to capture, store, map, analyze, preserve, control access to, integrate, and present evidence. |
| Ext17 | .424 | Controls security information through dashboards and metrics that continuously and dynamically measure information security performance. |
| Ext25 | .388 | A documented system security architecture configuration with consistent standards throughout the entire platform. |

Table 51. Extant Policing (POLI)

| **Policing** | | |
|---|---|---|
| **Cronbach's Alpha 0.870**<br>**Variance 8.3%** | | |
| **Var** | **Load** | **Question** |
| Ext22 | .654 | Policies clarifying the roles and tasks to comply with statutory and/or governmental regulations (e.g. Sarbanes–Oxley, HIPAA, admissibility rules, reporting requirements, international law, and penalties for security incidents). |
| Ext20 | .623 | Policies clarifying ownership of data in corporate and personnel devices, use of systems, privacy, and consent of monitoring. |
| Ext21 | .536 | Policies defining potential incidents and how to respond to them. |
| Ext32 | .509 | Procedures describing the configuration and use of active monitoring and logging mechanisms, including procedures to prevent alteration of intercepted communications. |
| Ext24 | .506 | A quality assurance system, with good records, that covers policies, activities, procedures, training, roles, documentation, and management. |
| Ext16 | .379 | Develops corporate policies and procedures collaboratively using collaboration tools to maintain a shared workspace. |

Table 52. Extant Active Control (ACON)

| **Active Control** | | |
|---|---|---|
| **Cronbach's Alpha 0.807**<br>**Variance 7.2%** | | |
| **Var** | **Load** | **Question** |
| Ext11 | .658 | Bans disk scrubbing tools, file shredding software, personal file encryption, and anti-forensic strategies (e.g. anonymity, data destruction/alteration, and onion routing). |
| Ext14 | .623 | Profiles and monitors systems' users and their personal devices. |
| Ext15 | .584 | Controls physical access to, classifies, and relocates corporate physical and digital assets according to a digital forensic program. |
| Ext19 | .506 | Performs security benchmarking to assess the preparedness of competitors and enemies. |

Table 53. Extant Backup Resourcing (BACK)

| **Backup Resourcing** | | |
|---|---|---|
| **Cronbach's Alpha 0.699**<br>**Variance 4.9%** | | |
| **Var** | **Load** | **Question** |
| Ext42 | .615 | Multiple virtual locations, wired and wireless networks, and/or a mobile platform. |
| Ext41 | .572 | Storage technology that is appropriate in capacity and functionality, including storage visualization abilities. |
| Ext34 | .539 | Procedures for performing backups, gathering permanent and volatile data, and analyzing admissible evidence. |
| Ext43 | .525 | Enough funding for the implementation of digital forensic readiness. |

Table 54. Extant Wireless Accessibility (WIRE)

| **Wireless Accessibility** | | |
|---|---|---|
| **Cronbach's Alpha N/A**<br>**Variance 2.2%** | | |
| **Var** | **Load** | **Question** |
| Ext3 | .918 | Allows wireless access. |

### Conceptual Model from EFA

In light of the findings and the conceptual analysis, the DFR model consists of eight extant and six perceptual factors. The extant factors, representing 53 variables, define what DFR is, according to the literature. The perceptual factors, representing 18 variables, should reflect the DFR status as defined by the extant factors. This is depicted by the following model where ovals represent the extant and perceptual DFR constructs and rectangles represent the latent factors that comprise the extant DFR, on one side, and those which reflect the perceptual DFR, on the other. The small squares indicate the number of variables loading on each factor. The demographic variables have not yet been included in the analysis.

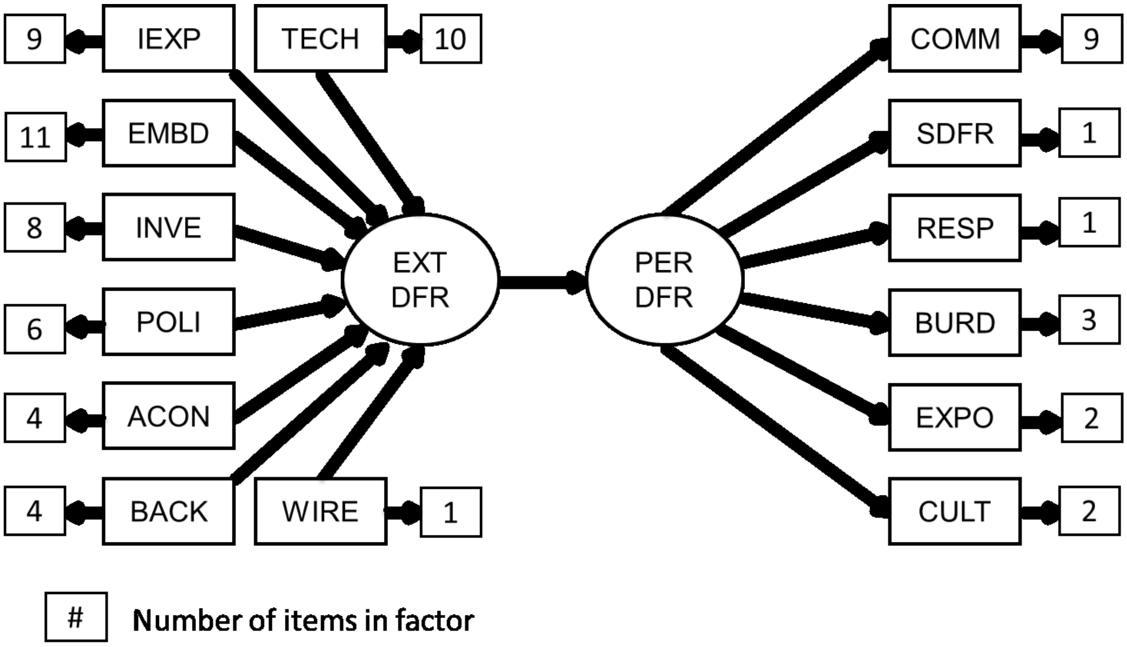


Figure 9. Conceptual model from exploratory factor analysis

### Demographic Variables

Demographic variables were not included in the factor analysis. Even though they can be considered extant conditions, they do not correspond to things that the organization has, does or knows; hence, it would be inappropriate to include them in the EFA. Nevertheless, this study found five relevant characteristics supported by the literature that can eventually affect DFR. Four of the demographic variables are continuous and refer to the size of the organization, i.e., Yearly Sales, Number of Employees, Number of Customers, and Amount of Data produced in a month. The fifth demographic variable nominally identifies the industry to which the organization belongs. One way to assess these variables effect is to develop a composite measure of extant DFR and use it as the dependent variable in a regression on them.

This research recommends that future researchers use summated scales for each factor, thus, including, only and equally, each one of their respective indicators with significant loadings. However, the factors' impact on the Extant or Perceived DFR constructs should not be treated equally because variables in factors defined by few variables would have a larger impact than the variables in factors defined by many variables. For example, the variable defining the Perceived Response Control factor would have nine times the weight of a variable in the Perceived Organizational Commitment factor. A more conservative approach would be to give an equal weight to each variable and calculate a composite Extant DFR and a composite Perceived DFR. By running a multiple regression of the composite Extant DFR on the four continuous organizational demographic variables (i.e., Sales, Number of Employees, Number of Customers and Amount of Data), a significant effect of the Number of Employees on the Extant DFR (p value = .006) is obtained. The other demographics are not significant when considering all these variables in the model. This is shown in the following table where the significant variable DemEmp is highlighted with a gray background.

Table 55. Test for Continuous Demographic Variables

**Coefficients**[a]

| Model | | Unstandardized Coefficients | | Standardized Coefficients | T | Sig. | 95.0% Confidence Interval for B | |
|---|---|---|---|---|---|---|---|---|
| | | B | Std. Error | Beta | | | Lower Bound | Upper Bound |
| 1 | (Constant) | 2.88 | 0.187 | | 15.393 | 0 | 2.511 | 3.248 |
| | DemSal | -0.023 | 0.042 | -0.043 | -0.549 | 0.584 | -0.105 | 0.059 |
| | DemEmp | -0.112 | 0.041 | -0.223 | -2.764 | 0.006 | -0.192 | -0.032 |
| | DemCus | 0.024 | 0.044 | 0.042 | 0.542 | 0.588 | -0.062 | 0.11 |
| | DemDat | -0.073 | 0.054 | -0.108 | -1.361 | 0.175 | -0.178 | 0.033 |

a. Dependent Variable: EXTDFR

This suggests that the number of employees could be a predictor of EXTDFR, although in the opposite direction inferred from the literature. Even though "a higher number of employees increase the risks for criminal incidents" (Barske et al. 2010), this condition might create awareness of the risks and make organizations take measures to counter those risks and be more prepared for them. Also, bigger organizations are more likely to count among their employees some with the qualifications required for DFR.

Further, a multiple covariate ANCOVA test is run to test the effect of the industry to which the organization belongs. Barske et al. (2010) suggest that financial firms might have a higher incidence of criminal activity than other firms. Thus, a dummy variable separating financial institutions from organizations in other industries was created and used as the variable of interest. The other organizational demographic variables are used as covariates. This test was not significant for the impact of Industry. The appropriateness of this test was validated by a test of homogeneity of variance based on median, which resulted in failing to reject the equality of the variance of the residuals in the two groups. The number of covariates satisfies Huitema's (1980) suggestion of being less than 0.1 * N - J + 1, where J is the number of groups and N, the sample size.

Table 56. Test for Nominal Demographic Variable

**Tests of Between-Subjects Effects** (DemInd6 = 1[b])

Dependent Variable: EXTDFR

| Source | Type III Sum of Squares | df | Mean Square | F | Sig. |
|---|---|---|---|---|---|
| Corrected Model | 9.406[a] | 5 | 1.881 | 4.731 | 0 |
| Intercept | 63.895 | 1 | 63.895 | 160.685 | 0 |
| DemSal | 0.114 | 1 | 0.114 | 0.288 | 0.592 |
| DemEmp | 2.987 | 1 | 2.987 | 7.512 | 0.007 |
| DemCus | 0.132 | 1 | 0.132 | 0.333 | 0.564 |
| DemDat | 0.737 | 1 | 0.737 | 1.855 | 0.175 |
| DemInd6 | 0.113 | 1 | 0.113 | 0.284 | 0.594 |
| Error | 97.024 | 244 | 0.398 | | |
| Total | 1277.562 | 250 | | | |
| Corrected Total | 106.43 | 249 | | | |

a. R Squared = .088 (Adjusted R Squared = .070)
b. Dummy variable for the sixth choice of Industry (Finance) = 1

Notwithstanding, applying a more sophisticated analysis such as SEM is recommended in the future in order to obtain a more precise picture of the interactions of the constructs, factors and indicators proposed herein.

### Testing Awareness

This research took an additional step by directly asking its respondents about their perception of the DFR status in their organizations. This question was asked twice, at the beginning and at the end of the survey, to take into account the effect of the survey as a mechanism that creates awareness of the construct. If a significant difference is detected between the pre- and post-survey perception of DFR, then, the survey itself affects this perception. Otherwise, we can think that respondents already had a clear idea of what the DFR status was in their organizations. By running a t-test it is found that the mean for both PER1 and PER18 is the same, 3.52. Their Pearson correlation is 0.762, showing high consistency between them along respondents. The survey, then, does not seem to have an effect on respondents' answers. This effect may change if subjects not as qualified as those surveyed in this research are recruited. Otherwise, the instrument has shown good potential to be deployed again as it is.

Given that PER1 and PER18 are asking the exact same question at different times, it was estimated appropriate to move PER18 to the Summary of DFR Assessment factor in the final model.

# CHAPTER V

# CONCLUSIONS

The Employees variable, conceptualy affecting the Extant DFR, was found significant; hence, the complete DFR framework should include this variable. However, running independent regressions for each of the organization size variables shows that thay all are significant predictors of DFR. Therefore, it is reasonable to think that organization size is the broader factor affecting DFR and Number of Employees is the proxy variable to which this factor can be reduced. This conceptual approach is visually represented by creating a box for the Organization Size factor which contains the proxy variable Number of Empoyees.

This demographic factor, although an existent condition, is of a different nature from the extant variables and, thus, not expected to be part of the components of DFR. The exact relationship between this and the extant factors should be the subject of future studies. The present model places the Organization Size factor apart from the extant factors to emphasize the difference.

The relationships among the Extant and Perceptual factors within their repective groups are also to be defined by future research as many different configurations can be devised from this initial framework. Given that the information currently used for exploratory purposes should not be used to confirm proposed models, those configurations must be theoretically supported and tested on new data.

However, an additional step can be pursued by running a second order factor analysis on the factors already found. Because the factors have been chosen so they are orthogonal, the correlations among them resulting from the new factor analysis are low. The MSA KMO indicators are 0.50 and 0.532 for the Extant and Perceptual variables sets respectively, which are considered not adequate for factor analysis. Still, one point of attention is that the perceptual factors are considered as reflective of DFR; therefore, they should move together reflecting changes in DFR. However, the low correlations among them, as shown below, do not support this assumption.

Table 57. Correlations among Perceptual Factors

| Correlation Matrix | | | | | | |
|---|---|---|---|---|---|---|
| | COMM | SDFR | RESP | BURD | EXPO | CULT |
| COMM | 1.000 | .137 | .164 | -.021 | .025 | .127 |
| SDFR | .137 | 1.000 | .012 | -.037 | .082 | .130 |
| RESP | .164 | .012 | 1.000 | .084 | .028 | .099 |
| BURD | -.021 | -.037 | .084 | 1.000 | .163 | .080 |
| EXPO | .025 | .082 | .028 | .163 | 1.000 | .019 |
| CULT | .127 | .130 | .099 | .080 | .019 | 1.000 |

There could be different explanations for this to happen, from lacking perceptual variables that help define the perceptual factors to having a different configuration for the relationship of the factors with each other. Testing these hypotheses requires new data and must be undertaken in future studies. The framework proposed herein acknowledges this uncertainty by using a dotted box to enclose all perceptual factors within the Extant DFR construct.

Some of the factors found in the pilot study, such as those related to Commitment, Control, Policing, and Investigation, remain equally relevant in the present framework. Other factors from the pilot study have been condensed in the more consistent factors resulted from the final study.

### Conceptual Model of DFR

As a result of the previous considerations, a proposed framework of DFR is proposed including the demographic factor Organization Size measured through Number of Employees as a predictor of Extant DFR, distinct from the components extracted from the factor analysis. The model also depicts the fact that the Perceptual factors are yet to be statistically proven to be reflections of the latent construct Perceived DFR. The DFR framework developed in this study is represented by the following conceptual model:

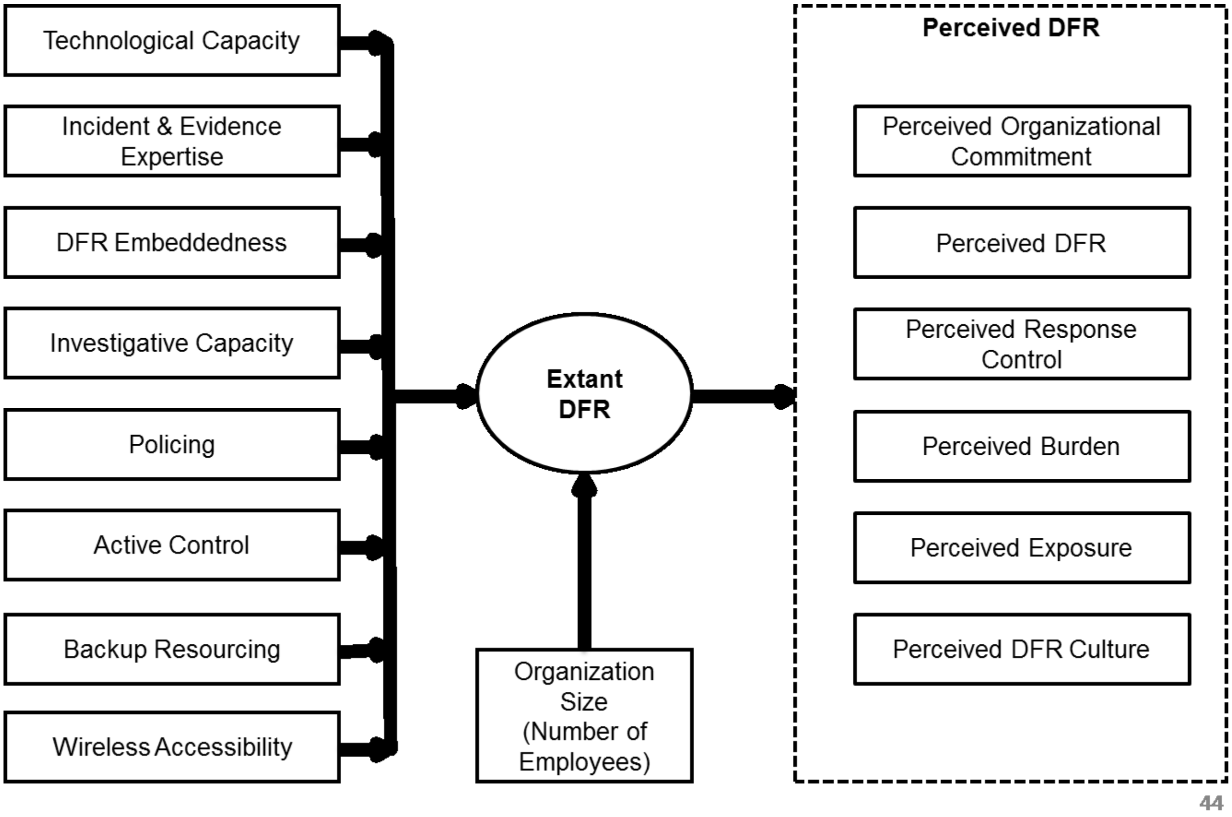


Figure 10. Conceptual model of DFR

The demographic, perceptual, and extant factors are explained in better detail in the following table:

Table 58. Definition of factors

**Demographic Factor**

**Number of Employees**

This is the only demographic factor that showed some effect in the extant DFR and is a simple count of the number of employees in the organization.

**Perceptual Factors**

**Perceived Organizational Commitment**

This factor represents the commitment of the managers and all personnel with the digital forensics program reflected in the knowledge of the personnel and the consistency of the DFR program with the corporate objectives and the employees’ privacy.

**Summary of DFR Assessment**

This factor is a straightforward assessment of the general perception of DFR before and after the application of the survey. Although the pos-survey variable loaded higher in factor one, it also loads higher in this factor, where it is conceptually considered to belong.

**Perceived Response Control**

This factor captures the ability of the organization to balance the benefits of the investigation with its costs, as perceived by their personnel.

**Perceived Burden**

This factor explores aspects that can be perceived as obstacles for the implementation of DFR measures, such as legal requirements, the location of the firm, and the costs associated to the DFR program.

**Perceived Exposure**

This factor detects the organization’s personnel feelings of being exposed to attacks, for example, by disgruntled employees or for having a public profile or given the nature of the firm activities.

**Perceived DFR Culture**

This factor assesses the perception that a culture exists in favor of preserving evidence and keeping up to date knowledge of DFR.

**Extant Factors**

**Technological Capacity**

This extant factor evaluates the DFR capacities of the organization in terms of digital and physical infrastructure, systems, software, hardware, tools, training, monitoring, and qualified consultancy.

**Incident & Evidence Expertise**

This factor explores the knowledge of the organization personnel about the sources and qualifiers of data; the identification, causes and consequences of incidents; the people involved and the incident; and the appropriate tools and techniques to investigate and manage potential evidence in order to demonstrate due diligence.

**DFR Embeddedness**

This factor examines the extent to which the DFR program and practices are part of the corporate plans, processes, and systems, as well as customary in people's behaviors.

**Investigative Capacity**

This factor evaluates whether the organization has the infrastructure and specialized personnel to perform digital investigations.

**Policing**

This factor assesses the completeness and adequacy of corporate policies regarding regulatory compliance, accessibility to network and resources, ownership of data, use of systems and tools, expectations of privacy, and incident management.

**Active Control**

This factor evaluates the actions taken by the organization in order to control access to its systems and facilities, and the use of anti-forensic strategies and tools.

**Backup Resourcing**

This factor examines the financial, physical and digital resources for the storage and analysis of data.

**Wireless Accessibility**

This factor measures to what extent wireless access to the corporate resources is available.

## Assumptions and Limitations

The assessment of digital forensic readiness (DFR) has proven to be a complex endeavor. Many variables are involved and only the occurrence of an event can truly unveil the preparedness of an organization to collect, analyze, preserve and provide digital evidence about it. In addition, practical rather than theoretical literature is available for the exploration of this construct from a quantitative stand point.

In response to these limitations, this study decided to obtain information about DFR indicators from what is assumed to be the most qualified source: the academic literature. It is assumed here that this literature represents what defines the construct in a comprehensive way. On the other hand, the collection of data from organizations assumed that IT professionals in those organizations are knowledgeable enough to represent the DFR characteristics of those organizations.

Consequently, the Extant DFR proposed is assumed to be a comprehensive measure of DFR. On the other hand, given the limited availability of research exploring perceptual or behavioral aspects of DFR, some perceived factors should be seen with caution as more indicators are needed for their assessment. Still, the perceived organizational commitment and perceived DFR factors found here show good measures of reliability.

There are also limitations in terms of the generalizability of this study. Because this is the first and, heretofore, only statistically supported framework of the DFR construct, it is difficult to provide solid assessments of nomological validity; rather new researchers will benefit from this study to make it a reference for the assessment of the validity of their own DFR proposals. More research must be done to validate the scales and framework proposed herein. Likewise, data from different geographic regions outside the United States should be collected in order to prove the appropriateness of the framework in other contexts. Moreover, in the current rapidly evolving technological environment, it is expected that some aspects of the framework will need to be adjusted to these changes.

## Contribution and Directions for Future Research

This research has undertaken the assessment of DFR by reviewing all DFR-related literature that was found until 2015 and methodically distilling potential indicators of DFR in organizations. This process has included a variety of qualitative and quantitative techniques for the classification and quantification of dimensions, factors and indicators, such as semantic analisis, Q-Sort tests, association rules, and exploratory factor analysis.

The approach of the study has been inductive rather than deductive, thereby building theory rather than testing. However, the exercise of regressing the proposed composite perceived DFR on the proposed composite extant DFR produces a significant p value below 0.0005 with an adjusted R-Square of 0.746. The results are, then, encouraging, not only in terms of the assessment of DFR, but also in terms of the feasibility of developing a methodology to quantify a construct whose quantification has been elusive heretofore.

In the process, several contributions have been provided to the discipline of digital forensics, to the field of information systems and to the social sciences, in general. The three most general of these contributions are:

- Providing a practitioners' framework for the assessment of DFR;
- Providing the first quantitative approach to measure the DFR construct;
- Proposing an innovative methodology for the structured assessment of unstructured problems, such as measuring DFR and other qualitatively-treated constructs.

These contributions have complementary but distinct implications for practitioners and academics.

### Implications for Practice

In first place, this study delivered a practitioner's framework of DFR that allows professionals to focus, in a systematic way, on the aspects that are more relevant in the evaluation of DFR in organizations. The dimensions proposed refer to entities that must be easily recognized by practitioners of IT security and digital forensics. Likewise, the indicators represent actions and conditions associated to those entities in a straightforward fashion.

The practitioner's framework proposed in Table 10 has not been subjected to statistical validation. Therefore, some demographic variables later found not to be significant predictors of the Extant DFR remain in the framework. This was purposely done because these variables have support from the literature and should not be discarded in real assessments of DFR. Practitioners can, instead, accumulate data on their real assessments in order to prove or disprove the relevance of such variables. Also, some indicators inferred to be negatively correlated to the Extant DFR variable, such as the culture of secrecy, the firm’s location, and the cost of the forensic program seem to be, instead, positively correlated to it.

One possible cause of this lies in the wording of the question or the interpretation of the respondents in the final survey. Another, perhaps, more plausible cause, is that those external elements seen as particular disadvantages for a firm make it more proactive in implementing measures that strengthen its DFR posture. For example, keeping the DFR program secret from employees might not be good for DFR, while keeping it secret from external agents, could be. This will require the practitioner to be cautious in the inquiries and diligent in the interpretation of responses.

The framework is not aimed to be a deterministic predictor of DFR but rather a structured tool through which DFR assessments can be compared and improved. Practitioners should use the framework as a guide to perform an organized assessment of DFR but be active in the interpretation of the results.

### Implications for Research

The second outcome of this study offers a conceptual model separating what can be considered as a status of DFR from the perceptions reflecting that status. This model is more appropriate for academics and researchers, who would benefit from the statistically supported framework in order to advance in the investigation of the construct. More research is needed, especially in the assessment of the Perceptual DFR. Likewise, replication of the study can help confirm the consistency of the Extant DFR factors. Additionally, new trends and technologies, such as blockchain and the Internet of Things (IoT), which were not mentioned as potential indicators of DFR status, should be included in future explorations of the DFR construct. New research should work on the confirmatory power of the framework and its continuous refinement.

Future research is expected to focus on the improvement of the scales of indicators for each factor and on each factor’s impact on the final status of DFR. The suggestion, then, is to find an alternative measure of DFR against which these factors could be compared. It is also recommended that specific indicators for those new factors are developed. New data should be collected to run a confirmatory analysis and, further, a structural equation model of this framework. Researchers should also provide guidelines for practitioners along the lines of Capability Maturity Models where real or ideal organizations at different levels of DFR can be used as examples to compare and contrast the status of those ones under evaluation.

As an additional contribution, this study has implemented innovative modifications to the application of the Q-Sort test and association rules algorithms that have demonstrated not only their usefulness, but the potential for new implementations of these techniques. Furthermore, this study provides an approach for the whole process of providing structure to an essentially unstructured problem, such as the assessment of DFR. This process can be summarized as the comprehensive review of the literature available on the construct, the identification of potential indicators, the classifications and refinement of those indicators, and the exploration of the latent factors explaining those variables and their relationships. Researchers in the social sciences are encouraged to use and test this approach to help building structured methodologies for the assessment of the plethora of elusive constructs in our disciplines.

# LIST OF REFERENCES

Ahmad, A. (2002, September). The forensic chain of evidence model: Improving the process of evidence collection in incident handling procedures. 6th Pacific Asia Conference on Information Systems.

Alharbi, S., Weber-Jahnke, J., & Traore, I. (2011). The proactive and reactive digital forensics investigation process: A systematic literature review. Information Security and Assurance (pp. 87-100). Springer Berlin Heidelberg.

Barske, D., Stander, A. & Jordan, J. (2010) “A digital forensic readiness framework for South African SME’s”. Information Security for South Africa (ISSA), pages 1-6. Sandton, Johannesburg: IEEE.

Beebe, N. (2009). Digital forensic research: The good, the bad and the unaddressed. In *Advances in digital forensics V* (pp. 17-36). Springer Berlin Heidelberg.

Beebe, N. L., & Clark, J. G. (2005). A hierarchical, objectives-based framework for the digital investigations process. *Digital Investigation*, *2*(2), 147-167.

Bem, D., Feld, F., Huebner, E., & Bem, O. (2008). Computer Forensics-Past, Present and Future. Journal of Information Science and Technology, 5(3), 43-59.

Bradford, P. G., Brown, M., Perdue, J., & Self, B. (2004, April). Towards proactive computer-system forensics. In Information Technology: Coding and Computing, 2004. Proceedings. ITCC 2004. International Conference on (Vol. 2, pp. 648-652). IEEE.

Brezinski & Killalea (Feb. 2002) Guidelines for Evidence Collection and Archiving http://www.hjp.at/doc/rfc/rfc3227.html and http://tools.ietf.org/html/rfc3227.

Carrier, B., & Spafford, E. H. (2004, July). An event-based digital forensic investigation framework. In Digital forensic research workshop (pp. 11-13).

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

Casey, E. (2006). Investigating sophisticated security breaches. Communications of the ACM, 49(2), 48-55.

Casey, E. (2005). Case study: network intrusion investigation–lessons in forensic preparation. *Digital Investigation*, *2*(4), 254-260.

Chen, P. S., Tsai, L. M., Chen, Y. C., & Yee, G. (2005, November). Standardizing the construction of a digital forensics laboratory. In *Systematic Approaches to Digital Forensic Engineering, 2005. First International Workshop on* (pp. 40-47). IEEE.

Chin, W. W., Johnson, N., & Schwarz, A. (2008). A fast form approach to measuring technology acceptance and other constructs. MIS Quarterly, 687-703.

Chris Prosise and Kevin Mandia. Incident Response: Investigating Computer Crime. McGrawHill Osborne Media, 2001.

Ciardhuáin, S. Ó. (2004). An extended model of cybercrime investigations.International Journal of Digital Evidence, 3(1), 1-22.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS quarterly*, 319-340.

Danielsson, J., & Tjøstheim, I. (*2004).* The Need for a Structured Approach to Digital Forensic Readiness. *E-Commerce*, 417.

Duranti, L., & Endicott-Popovsky, B. (2010). Digital records forensics: A new science and academic program for forensic readiness. Journal of Digital Forensics, Security and Law, 5(2), 45-62.

Elachgar, H., Boulafdour, B., Makoudi, & M., Regragui, B. (2012). Information security, 4th wave. Journal of theoretical and applied information technology, 43(2).

Elyas, M., Ahmad, A., Maynard, S. B., & Lonie, A. (2015). Digital forensic readiness: Expert perspectives on a theoretical framework. *Computers & Security*, *52*, 70-89.

Elyas, M., Maynard, S. B., AHMAD, A., & Lonie, A. (2014). Towards A Systemic Framework Of Forensic Readiness. *Journal of Computer Information Systems*, *54*(3).

Endicott-Popovsky, B., Frincke, D. A., & Taylor, C. A. (2007). A theoretical framework for organizational network forensic readiness. Journal of Computers,2(3), 1-11.

Ferguson-Boucher, K., & Endicott-Popovsky, B. (2012). Forensic Readiness in the Cloud (FRC): Integrating Records Management. Cybercrime and Cloud Forensics: Applications for Investigation Processes: Applications for Investigation Processes, 105.

Forrester, J., & Irwin, B. (2007). A Digital Forensic investigative model for business organisations. *IFIPSec 2007*.

Forte, D. V. (2010). The responsibilities of an incident responder. Network Security, 2010(1), 18-19.

Garfinkel, S. L. (2010). Digital forensics research: The next 10 years. *digital investigation*, *7*, S64-S73.

Grobler, C. P., & Louwrens, C. P. (2007, May). Digital forensic readiness as a component of information security best practice. In IFIP International Information Security Conference (pp. 13-24). Springer US.

Grobler, C. P., Louwrens, C. P., & von Solms, S. H. (2010, February). A framework to guide the implementation of proactive digital forensics in organisations. In Availability, Reliability, and Security, 2010. ARES'10 International Conference on (pp. 677-682). IEEE.

Grobler, C. P., Louwrens, C. P., & von Solms, S. H. (2010, February). A multi-component view of digital forensics. In *Availability, Reliability, and Security, 2010. ARES'10 International Conference on* (pp. 647-652). IEEE.

Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2010). Multivariate data analysis: A global perspective. Pearson Education.

Hamidovic, H. (Feb. 2012). Digital Forensic Readiness. Internal Auditor (ITAudit), p. 23.

Hoolachan, S. A., & Glisson, W. B. (2010, May). Organizational handling of digital evidence. In Proceedings of the Conference on Digital Forensics, Security and Law (pp. 33-44).

Huitema, B. (1980). The analysis of covariance and alternatives Wiley. New York.Kaiser, H. F. (1974). An index of factorial simplicity. Psychometrika, 39(1), 31-36.

Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). Guide to integrating forensic techniques into incident response. Recommendations of the National Institute of Standards and Technology. Special Publication 800–86. National Institute of Standards and Technology: Gaithersburg.

Kroenke, D. M., & Hooper, T. (2011). *Using Mis*. Pearson.

Kruse II, W. G., & Heiser, J. G. (2002). Computer forensics: incident response essentials. Pearson Education. In library QA76.9.A25 K78 2002 ISBN 0201707195 LCCN: 2001034106.

Khurana, H., Basney, J., Bakht, M., Freemon, M., Welch, V., & Butler, R. (2009, April). Palantir: a framework for collaborative incident response and investigation. In Proceedings of the 8th Symposium on Identity and Trust on the Internet (pp. 38-51). ACM.

Leigh, V. (2012). Why you need to get to know your IT Department now. Six simple steps to improve emergency response planning and litigation readiness. Travel Law Quarterly, 4(3), 236-239.

Luoma (2006). Computer forensics and electronic discovery: The new management challenge, Computers and Security, vol. 25(2), pp. 91–96.

Maconachy, W. V., Schou, C. D., Ragsdale, D., & Welch, D. (2001, June). A model for information assurance: An integrated approach. In Proceedings of the 2001 IEEE Workshop on Information Assurance and Security (Vol. 310). New York, USA.

Mandia, K., Prosie, C, & Pepe, M. (2003). Incident Responses Computer Forensics, Second Edition (2nd ed). Emeryville, CA: McGraw-Hill/Osborne.

Mouhtaropoulos, A., Dimotikalis, P., & Li, C. T. (2013, November). Applying a digital forensic readiness framework: three case studies. In Technologies for Homeland Security (HST), 2013 IEEE International Conference on (pp. 217-223). IEEE.

Mouhtaropoulos, A., Li, C., & Grobler, M. (2012). Proactive Digital Forensics: The Ever-Increasing Need for Standardization. 2012 European Intelligence & Security Informatics Conference, 289. doi:10.1109/EISIC.2012.66

Mouhtaropoulos & C. Li, (2012). Forensic Readiness Framework Components : a Preliminary Approach. Contemporary Private Law, vol. 4, no. 2, Kierkegaard Sylvia, Ed. 2012.

Mouhtaropoulos, A., Grobler, M., & Li, C. T. (2011, September). Digital forensic readiness: an insight into governmental and academic initiatives. In Intelligence and Security Informatics Conference (EISIC), 2011 European (pp. 191-196). IEEE.

Mouton, Francois, and H. S. Venter. "A prototype for achieving digital forensic readiness on wireless sensor networks." *AFRICON, 2011*. IEEE, 2011.

Ngobeni, S., Venter, H., & Burke, I. (2010). A forensic readiness model for wireless networks. In *Advances in Digital Forensics VI* (pp. 107-117). Springer Berlin Heidelberg.

Olavsrud, T. (2010, Dec. 14).  5 Information Security Trends That Will Dominate 2015. CIO.com. Retrieved in 2015-01-12 from http://www.cio.com/article/2857673/security0/5-information-security-trends-that-will-dominate-2015.html?page=3.

Pangalos, G., Ilioudis, C., & Pagkalos, I. (2010, June). The importance of Corporate Forensic Readiness in the information security framework. In Enabling Technologies: Infrastructures for Collaborative Enterprises (WETICE), 2010 19th IEEE International Workshop on (pp. 12-16). IEEE.

Pangalos, G., & Katos, V. (2010). Information Assurance and Forensic Readiness. Next Generation Society. Technological and Legal Issues (pp. 181-188). Springer Berlin Heidelberg.

Pollitt, M. M. (2007, April). An ad hoc review of digital forensic models. In *Systematic Approaches to Digital Forensic Engineering, 2007. SADFE 2007. Second International Workshop on* (pp. 43-54). IEEE.

Pooe, A., & Labuschagne, L. (2012, August). A conceptual model for digital forensic readiness. In Information Security for South Africa (ISSA), 2012 (pp. 1-8). IEEE.

Prosise, C., & Mandia, K. (2001). Incident Response : Investigating Computer Crime. New York: Osborne/McGraw-Hill.

Quinn, S. (2005). Examining the state of preparedness of Information Technology management in New Zealand for events that may require forensic analysis. Digital Investigation, 2(4), 276-280.

Reddy, K., Venter, H. S., & Olivier, M. S. (2012). Using time-driven activity-based costing to manage digital forensic readiness in large organisations.Information Systems Frontiers, 14(5), 1061-1077.

Reddy, K., & Venter, H. (2009). A forensic framework for handling information privacy incidents. In Advances in Digital Forensics V (pp. 143-155). Springer Berlin Heidelberg.

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

Reith, M., Carr, C., & Gunsch, G. (2002). An examination of digital forensic models. International Journal of Digital Evidence, 1(3), 1-12.

Richard, K. D. (1999). Electronic Evidence: To Produce or Not to Produce, That Is the Question. Whittier L. Rev., 21, 463.

Rogers, M. K., Goldman, J., Mislan, R., Wedge, T., & Debrota, S. (2006). Computer forensics field triage process model. Journal of Digital Forensics, Security and Law, 1(2), 19-38.

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

Schneier, B., & Kelsey, J. (1999). Secure audit logs to support computer forensics. ACM Transactions on Information and System Security (TISSEC),2(2), 159-176.

Serra, S. M., & Venter, H. S. (2011, August). Mobile cyber-bullying: A proposal for a pre-emptive approach to risk mitigation by employing digital forensic readiness. In *Information Security South Africa (ISSA), 2011* (pp. 1-5). IEEE.

Shedden, P., Ahmad, A., & Ruighaver, A. B. (2010). Organisational learning and incident response: promoting effective learning through the incident response process.

Starkman, P. (2014). Data breaches on the rise: Are you prepared to stop the leak in 2015?. Multibriefs. Retrieved in 2015-01-12 from http://exclusive.multibriefs.com/content/data-breaches-on-the-rise-are-you-prepared-to-stop-the-leak-in-2015/business-management-services-risk-management.

Stephenson, P. (2003). A comprehensive approach to digital incident investigation. Information Security Technical Report, 8(2), 42-54.

Spyridopoulos, T., & Katos, V. (2011). Requirements for a forensically ready cloud storage service. *International Journal of Digital Crime and Forensics (IJDCF)*, *3*(3), 19-36.

Tan, J. Forensic Readiness. Technical report, @stake, 2001. [28] Brent Turvey. Criminal Profiling: An Introduction to Behavioral Evidence Analysis. Academic Press, 2 edition, 2002.

Tan, T., Ruighaver, A. B., & Ahmad, A. (2003, November). Incident Handling: Where the need for planning is often not recognised. In Proceedings of the 1st Australian Computer Network, Information & Forensics Conference, Australia.

Taylor, M., Haggerty, J., Gresty, D., & Lamb, D. (2011). Forensic investigation of cloud computing systems. *Network Security*, *2011*(3), 4-10.

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

Trenwith, P. M., & Venter, H. S. (2013, August). Digital forensic readiness in the cloud. In Information Security for South Africa, 2013 (pp. 1-5). IEEE.

Valjarevic, A., & Venter, H. S. (2011, August). Towards a digital forensic readiness framework for public key infrastructure systems. In *Information Security South Africa (ISSA), 2011* (pp. 1-10). IEEE.

Van Staden, F., & Venter, H. (2012). Implementing Forensic Readiness using performance monitoring tools. In *Advances in Digital Forensics VIII* (pp. 261-270). Springer Berlin Heidelberg.

Van Staden, F. R., & Venter, H. S. (2011, August). Adding digital forensic readiness to electronic communication using a security monitoring tool. In*Information Security South Africa (ISSA), 2011* (pp. 1-5). IEEE.

Van Staden, F. R., & Venter, H. S. (2010, August). Adding digital forensic readiness to the email trace header. In *Information Security for South Africa (ISSA), 2010* (pp. 1-4). IEEE.

Von Solms, B. (2006). Information security - the fourth wave. Computers & security, 25(3), 165-168.

Von Solms, S., Louwrens, C., Reekie, C., & Grobler, T. (2006). A control framework for digital forensics. In Advances in Digital Forensics II (pp. 343-355). Springer New York.

Webb, J., Ahmad, A., Maynard, S. B., & Shanks, G. (2014). A situation awareness model for information security risk management. *Computers & Security*, *44*, 1-15.

Wikipedia (2015). Dimension. Retrieved from http://en.wikipedia.org/wiki/Dimension_(data_warehouse) and http://en.wikipedia.org/wiki/Dimension on May 31, 2015.

Wikipedia (2015). Factor. Retrieved from http://en.wikipedia.org/wiki/Factor on May 31, 2015.

Wolfe-Wilson, J., & Wolfe, H. B. (2003). Management strategies for implementing forensic security measures. Information Security Technical Report, 8(2), 55-64.

Yasinsac, A., & Manzano, Y. (2001, June). Policies to enhance computer and network forensics. In Proceedings of the 2001 IEEE workshop on information assurance and security (pp. 289-295).

Youst, L. R., & Koh, H. L. (1997). Management and Discovery of Electronically Stored Information. Computer L. Rev. & Tech. J., 73.

# LIST OF APPENDICES

# APPENDIX A - POTENTIAL INDICATORS OF DFR FROM LITERATURE REVIEW

| Factor | Re-Classification | Paper Name | Year |
|---|---|---|---|
| Awareness of unknown risks | Factor | VonSolms 2000 / DIS ISO/IEC 17799 - 1 (BS 7799) | 2000 |
| Security policy | Dimension | VonSolms 2000 / DIS ISO/IEC 17799 - 1 (BS 7799) | 2000 |
| Security organization | Dimension | VonSolms 2000 / DIS ISO/IEC 17799 - 1 (BS 7799) | 2000 |
| Assets classification and control | Factor | VonSolms 2000 / DIS ISO/IEC 17799 - 1 (BS 7799) | 2000 |
| Personnel security | Dimension | VonSolms 2000 / DIS ISO/IEC 17799 - 1 (BS 7799) | 2000 |
| Physical and environmental security | Dimension | VonSolms 2000 / DIS ISO/IEC 17799 - 1 (BS 7799) | 2000 |
| Communications and operations | Dimension | VonSolms 2000 / DIS ISO/IEC 17799 - 1 (BS 7799) | 2000 |
| Management | Dimension | VonSolms 2000 / DIS ISO/IEC 17799 - 1 (BS 7799) | 2000 |
| Access control | Factor | VonSolms 2000 / DIS ISO/IEC 17799 - 1 (BS 7799) | 2000 |
| Systems development and maintenance | Dimension | VonSolms 2000 / DIS ISO/IEC 17799 - 1 (BS 7799) | 2000 |
| Business Continuity management | Dimension | VonSolms 2000 / DIS ISO/IEC 17799 - 1 (BS 7799) | 2000 |
| Compliance | Dimension | VonSolms 2000 / DIS ISO/IEC 17799 - 1 (BS 7799) | 2000 |
| Having International Information Security Certification | Factor | VonSolms 2000 | 2000 |
| Cultivating an Information Security Culture Right | Dimension | VonSolms 2000 | 2000 |
| Implementing Metrics to Continuously and Dynamically Measure IS aspects | Factor | VonSolms 2000 | 2000 |
| Management of People Leaving the Company | Factor | VonSolms 2000 | 2000 |
| Electronic Device type | Factor | US DoS/NIJ 2001 | 2001 |
| Tools & Equipment | Dimension | US DoS/NIJ 2001 | 2001 |
| Securing and Evaluating the Scene | Factor | US DoS/NIJ 2001 | 2001 |
| Documenting the Scene | Factor | US DoS/NIJ 2001 | 2001 |
| Evidence Collection | Dimension | US DoS/NIJ 2001 | 2001 |
| Packaging, Transportation, and Storage | Dimension | US DoS/NIJ 2001 | 2001 |
| Crime Category | Factor | US DoS/NIJ 2001 | 2001 |
| Ability to collect evidence | Factor | Tan 2001 | 2001 |
| Cost of forensics | Factor | Tan 2001 | 2001 |
| Multitiered logging | Factor | Tan 2001 | 2001 |
| How Logging is Done | Factor | Tan 2001 | 2001 |
| What is Logged | Factor | Tan 2001 | 2001 |
| Intrusion Detection Systems (IDS) | Factor | Tan 2001 | 2001 |

| | | | |
|---|---|---|---|
| Forensic Acquisition | Dimension | Tan 2001 | 2001 |
| Evidence Handling | Dimension | Tan 2001 | 2001 |
| Centralized logging | Factor | Tan 2001 | 2001 |
| Formatting data in a single format, such as syslog | Factor | Tan 2001 | 2001 |
| Logging time synchronization according to time-zones | Factor | Tan 2001 | 2001 |
| Accuracy of the time to which devices are synchronized | Factor | Tan 2001 | 2001 |
| Time-Stamping | Factor | Tan 2001 | 2001 |
| Permissions | Factor | Tan 2001 | 2001 |
| Trade-offs involved with IDS monitoring and reporting | Factor | Tan 2001 | 2001 |
| Liability vs. obligation in the retention of log data | Factor | Tan 2001 | 2001 |
| File System | Factor | Tan 2001 | 2001 |
| Integrity of NIDS log data | Factor | Tan 2001 | 2001 |
| Sitting of NIDS relative to an intruder | Factor | Tan 2001 | 2001 |
| Imaging and Backup | Factor | Tan 2001 | 2001 |
| Chain of custody | Dimension | Tan 2001 | 2001 |
| Transport and encryption | Dimension | Tan 2001 | 2001 |
| Physical storage & transport of evidence | Dimension | Tan 2001 | 2001 |
| Retaining Information. | Factor | Yasinsac & Manzano 2001 | 2001 |
| Do the organization copy and retain application and local user files? | Factor | Yasinsac & Manzano 2001 | 2001 |
| Do the organization copy and retain computer and network activity logs? | Factor | Yasinsac & Manzano 2001 | 2001 |
| Planning the response. | Dimension | Yasinsac & Manzano 2001 | 2001 |
| Does the organization have a forensic team? | Factor | Yasinsac & Manzano 2001 | 2001 |
| Does the organization have an intrusion response procedure? | Factor | Yasinsac & Manzano 2001 | 2001 |
| Is there a formal investigative procedure? | Factor | Yasinsac & Manzano 2001 | 2001 |
| Training. | Dimension | Yasinsac & Manzano 2001 | 2001 |
| Is there training for the response team? | Factor | Yasinsac & Manzano 2001 | 2001 |
| Is there training for the investigative team? | Factor | Yasinsac & Manzano 2001 | 2001 |
| Is there training on DF for all personnel that use computers? | Factor | Yasinsac & Manzano 2001 | 2001 |
| Accelerating the investigation. | Dimension | Yasinsac & Manzano 2001 | 2001 |
| Is personal file encryption prohibited? | Factor | Yasinsac & Manzano 2001 | 2001 |
| Is disk scrubbing tools and file shredding software prohibited? | Factor | Yasinsac & Manzano 2001 | 2001 |
| Are data indexes utilized? | Factor | Yasinsac & Manzano 2001 | 2001 |
| Is information fusion utilized? | Factor | Yasinsac & Manzano 2001 | 2001 |
| Prevent anonymous activities. | Factor | Yasinsac & Manzano 2001 | 2001 |

| | | | |
|---|---|---|---|
| Is onion routing prevented or used? | Factor | Yasinsac & Manzano 2001 | 2001 |
| Are date, time and user stamps in file required? | Factor | Yasinsac & Manzano 2001 | 2001 |
| Is strong user authentication used? | Factor | Yasinsac & Manzano 2001 | 2001 |
| Are strong access control mechanisms used? | Factor | Yasinsac & Manzano 2001 | 2001 |
| Protect the evidence. | Dimension | Yasinsac & Manzano 2001 | 2001 |
| Is there rigid control over access for systems housing potential evidence? | Factor | Yasinsac & Manzano 2001 | 2001 |
| Are evidence files and connections encrypted? | Factor | Yasinsac & Manzano 2001 | 2001 |
| Is there strong integrity checking technology? | Factor | Yasinsac & Manzano 2001 | 2001 |
| Information States | Dimension | Maconachy, Schou, Ragsdale & Welch 2001 | 2001 |
| Security Services | Dimension | Maconachy, Schou, Ragsdale & Welch 2001 | 2001 |
| Security Countermeasures | Dimension | Maconachy, Schou, Ragsdale & Welch 2001 | 2001 |
| Time | Dimension | Maconachy, Schou, Ragsdale & Welch 2001 | 2001 |
| Education | Dimension | Maconachy, Schou, Ragsdale & Welch 2001 | 2001 |
| Training. | Dimension | Maconachy, Schou, Ragsdale & Welch 2001 | 2001 |
| Literacy | Dimension | Maconachy, Schou, Ragsdale & Welch 2001 | 2001 |
| Awareness | Dimension | Maconachy, Schou, Ragsdale & Welch 2001 | 2001 |
| Reliable unbiased methods to extract and analyze evidence | Dimension | Reith, Carr & Gunch 2002 | 2002 |
| Standardization of procedures | Factor | Reith, Carr & Gunch 2002 | 2002 |
| Self education on new forensic technologies | Factor | Reith, Carr & Gunch 2002 | 2002 |
| Storage technology | Dimension | Reith, Carr & Gunch 2002 | 2002 |
| Chain of custody | Dimension | Reith, Carr & Gunch 2002 | 2002 |
| System, audit, application, and network management logs | Factor | Ahmad 2002 | 2002 |
| Network traffic capture | Factor | Ahmad 2002 | 2002 |
| Data regarding the state of the file system | Factor | Ahmad 2002 | 2002 |
| Centralization of loggins | Factor | Ahmad 2002 | 2002 |
| Physical access control logs or CCTV pictures | Factor | Ahmad 2002 | 2002 |
| Immediate physical work environment around the computer system | Factor | Ahmad 2002 | 2002 |
| Preserving Chain of evidence | Factor | Ahmad 2002 | 2002 |
| Record of user behavior within the boundaries of network application | Factor | Ahmad 2002 | 2002 |
| Interaction between network applications and the traffic they generate | Factor | Ahmad 2002 | 2002 |

|  |  |  |  |
|---|---|---|---|
| Documenting observations | Factor | Ahmad 2002 | 2002 |
| Links among timing of links, CCTV pictures, user identification logs, etc. | Factor | Ahmad 2002 | 2002 |
| Infrastructure digital and physical | Dimension | Carrier & Spafford 2003 | 2003 |
| Operations | Dimension | Carrier & Spafford 2003 | 2003 |
| Training | Dimension | Carrier & Spafford 2003 | 2003 |
| Equipment | Dimension | Carrier & Spafford 2003 | 2003 |
| Maintenance of the target environment | Dimension | Carrier & Spafford 2003 | 2003 |
| Event Log information | Factor | Chen, Clark, Devel & Mohay 2003 | 2003 |
| Remoteness of crimes | Factor | Stephenson 2003 | 2003 |
| Amount of data available to analyze | Factor | Stephenson 2003 | 2003 |
| What is the nature of the incident? | Factor | Stephenson 2003 | 2003 |
| How can we be sure that there even was an incident? | Dimension | Stephenson 2003 | 2003 |
| What was the entry point into the target system? Was there only one? | Factor | Stephenson 2003 | 2003 |
| What would evidence of an attack look like? What are we looking for? | Factor | Stephenson 2003 | 2003 |
| What legal issues need to be addressed (policies, privacy, subpoenas, warrants, etc.)? | Dimension | Stephenson 2003 | 2003 |
| Who was in a position to cause/allow the incident to occur? | Factor | Stephenson 2003 | 2003 |
| What security measures were in place at the time of the incident? | Factor | Stephenson 2003 | 2003 |
| What non-technical (business) issues impacted the success or failure of the attack? | Dimension | Stephenson 2003 | 2003 |
| Who knew what about the attack and when did they know it? (Stephenson 2003) | Factor | Stephenson 2003 | 2003 |
| Investigator background (Scientific vs. Practical) | Factor | Stephenson 2003 | 2003 |
| Technique - Whether the theory or technique can be and has been tested. | Factor | Stephenson 2003 / Daubert test | 2003 |
| Technique - Whether it has been subjected to peer review and publication. | Factor | Stephenson 2003 / Daubert test | 2003 |
| Technique - Its known potential rate of error & maintenance of controlling standards | Factor | Stephenson 2003 / Daubert test | 2003 |
| Technique - The degree of acceptance within the relevant scientific community. | Factor | Stephenson 2003 / Daubert test | 2003 |
| Logs from involved computers, detection systems, firewalls, etc. | Dimension | Stephenson 2003 / Daubert test | 2003 |
| A. Identification | Dimension | DFRWS cited by Stephenson 2003 | 2003 |
| A1. Event/Crime Detection | Factor | DFRWS cited by Stephenson 2003 | 2003 |

| | | | |
|---|---|---|---|
| A2. Resolve Signature | Factor | DFRWS cited by Stephenson 2003 | 2003 |
| A3. Profile Detection | Factor | DFRWS cited by Stephenson 2003 | 2003 |
| A4. Anomalous Detection | Factor | DFRWS cited by Stephenson 2003 | 2003 |
| A5. Complaints | Factor | DFRWS cited by Stephenson 2003 | 2003 |
| A6. System | Dimension | DFRWS cited by Stephenson 2003 | 2003 |
| A7. Monitoring Audit Analysis | Dimension | DFRWS cited by Stephenson 2003 | 2003 |
| B. Preservation | Dimension | DFRWS cited by Stephenson 2003 | 2003 |
| B1. Case Management | Dimension | DFRWS cited by Stephenson 2003 | 2003 |
| B2. Imaging Technologies | Factor | DFRWS cited by Stephenson 2003 | 2003 |
| B3. Chain of Custody | Dimension | DFRWS cited by Stephenson 2003 | 2003 |
| B4. Time Synchronization | Factor | DFRWS cited by Stephenson 2003 | 2003 |
| C. Collection | Dimension | DFRWS cited by Stephenson 2003 | 2003 |
| C1. Preservation | Dimension | DFRWS cited by Stephenson 2003 | 2003 |
| C2. Approved Methods | Dimension | DFRWS cited by Stephenson 2003 | 2003 |
| C3. Approved Software | Dimension | DFRWS cited by Stephenson 2003 | 2003 |
| C4.Approved Hardware | Dimension | DFRWS cited by Stephenson 2003 | 2003 |
| C5. Legal Authority | Dimension | DFRWS cited by Stephenson 2003 | 2003 |
| C6. Lossless Compression | Factor | DFRWS cited by Stephenson 2003 | 2003 |
| C7. Sampling | Factor | DFRWS cited by Stephenson 2003 | 2003 |
| C8. Data Reduction Recovery | Factor | DFRWS cited by Stephenson 2003 | 2003 |
| C9. Recovery Techniques | Factor | DFRWS cited by Stephenson 2003 | 2003 |
| D. Examination | Dimension | DFRWS cited by Stephenson 2003 | 2003 |
| D1. Preservation | Dimension | DFRWS cited by Stephenson 2003 | 2003 |
| D2. Traceability | Factor | DFRWS cited by Stephenson 2003 | 2003 |
| D3. Validation Techniques | Factor | DFRWS cited by Stephenson 2003 | 2003 |
| D4. Filtering Techniques | Factor | DFRWS cited by Stephenson 2003 | 2003 |
| D5. Pattern Matching | Factor | DFRWS cited by Stephenson 2003 | 2003 |
| D6. Hidden Data Discovery | Factor | DFRWS cited by Stephenson 2003 | 2003 |

|  |  |  |  |
|---|---|---|---|
| D7. Hidden Data Extraction | Factor | DFRWS cited by Stephenson 2003 | 2003 |
| E. Analysis | Dimension | DFRWS cited by Stephenson 2003 | 2003 |
| E1. Preservation | Dimension | DFRWS cited by Stephenson 2003 | 2003 |
| E2. Traceability | Dimension | DFRWS cited by Stephenson 2003 | 2003 |
| E3. Statistical | Factor | DFRWS cited by Stephenson 2003 | 2003 |
| E4. Protocols | Factor | DFRWS cited by Stephenson 2003 | 2003 |
| E5. Data Mining | Factor | DFRWS cited by Stephenson 2003 | 2003 |
| E6. Timeline | Dimension | DFRWS cited by Stephenson 2003 | 2003 |
| E7. Link | Factor | DFRWS cited by Stephenson 2003 | 2003 |
| E8. Spatial | Dimension | DFRWS cited by Stephenson 2003 | 2003 |
| F. Presentation | Dimension | DFRWS cited by Stephenson 2003 | 2003 |
| F1. Documentation | Dimension | DFRWS cited by Stephenson 2003 | 2003 |
| F2. Expert Testimony | Factor | DFRWS cited by Stephenson 2003 | 2003 |
| F3. Clarification | Factor | DFRWS cited by Stephenson 2003 | 2003 |
| F4. Mission Impact Statement | Factor | DFRWS cited by Stephenson 2003 | 2003 |
| F5. Recommended Countermeasure | Factor | DFRWS cited by Stephenson 2003 | 2003 |
| F6. Statistical Interpretation | Factor | DFRWS cited by Stephenson 2003 | 2003 |
| Lack of awareness of tangible and intangible benefits | Factor | Tan, Ruighaver & Ahmad 2003 | 2003 |
| Firm interest in prosecuting offenders | Factor | Tan, Ruighaver & Ahmad 2003 | 2003 |
| Industry | Factor | Tan, Ruighaver & Ahmad 2003 | 2003 |
| Confidence in the security systems | Factor | Tan, Ruighaver & Ahmad 2003 | 2003 |
| Managers awareness and kowledge of security investigations | Factor | Tan, Ruighaver & Ahmad 2003 | 2003 |
| Ability to recognize an incident | Factor | Tan, Ruighaver & Ahmad 2003 | 2003 |
| Regulatory penalties for security incidents | Factor | Tan, Ruighaver & Ahmad 2003 | 2003 |
| Forensic toolkit (e-camera, gloves, etc.) and equipment, forms and supplies | Factor | Wolfe 2003 | 2003 |
| Documenting the chain of evidence | Factor | Wolfe 2003 | 2003 |
| Management Example and Support of security | Factor | Wolfe-Wilson & Wolfe 2003 | 2003 |
| Codes of conduct and security policies | Dimension | Wolfe-Wilson & Wolfe 2003 | 2003 |
| Fiduciary, statutory or government regulations | Factor | Wolfe-Wilson & Wolfe 2003 | 2003 |

| | | | |
|---|---|---|---|
| Impact of previous security events | Factor | Wolfe-Wilson & Wolfe 2003 | 2003 |
| Budget | Factor | Wolfe-Wilson & Wolfe 2003 | 2003 |
| Politically sensitive or public embarrassment type incident | Factor | Wolfe-Wilson & Wolfe 2003 | 2003 |
| Threat of opportunist, criminal, competitor or disgruntled employee | Factor | Wolfe-Wilson & Wolfe 2003 | 2003 |
| Chain of evidence | Dimension | Wolfe-Wilson & Wolfe 2003 | 2003 |
| IDS, IPS, Network traffic and logs | Factor | Wolfe-Wilson & Wolfe 2003 | 2003 |
| Internal forensics group or external Computer Emergency Response Team - CERT | Factor | Wolfe-Wilson & Wolfe 2003 | 2003 |
| Laboratory and specialized hardware and software | Dimension | Wolfe-Wilson & Wolfe 2003 | 2003 |
| Audit that confirms good practices and tests the controls in place | Factor | Wolfe-Wilson & Wolfe 2003 | 2003 |
| Defining a risk mode | Factor | Wolfe-Wilson & Wolfe 2003 | 2003 |
| Following best practice security standards | Factor | Wolfe-Wilson & Wolfe 2003 | 2003 |
| Implementing good security products | Factor | Wolfe-Wilson & Wolfe 2003 | 2003 |
| Defining security policies and procedures | Factor | Wolfe-Wilson & Wolfe 2003 | 2003 |
| Training IT staff and educating users | Factor | Wolfe-Wilson & Wolfe 2003 | 2003 |
| Continually reviewing the security threats | Factor | Wolfe-Wilson & Wolfe 2003 | 2003 |
| Knowing and monitoring the organization’s IT infrastructure | Factor | Wolfe-Wilson & Wolfe 2003 | 2003 |
| Chain of custody | Dimension | Bradford, Brown, Perdue & Self 2004 | 2004 |
| Honey pots | Factor | Bradford, Brown, Perdue & Self 2004 | 2004 |
| Secrecy of proactive forensics system from users | Factor | Bradford, Brown, Perdue & Self 2004 | 2004 |
| Infrastructure | Dimension | Carrier & Spafford 2004 | 2004 |
| Preservation of physical and digital evidence | Dimension | Carrier & Spafford 2004 | 2004 |
| 1. Awareness (that investigation is needed) | Factor | Ciardhuáin 2004 | 2004 |
| 2. Authorisation (Legal or Managerial) | Factor | Ciardhuáin 2004 | 2004 |
| 3. Planning | Dimension | Ciardhuáin 2004 | 2004 |
| 4. Notification | Dimension | Ciardhuáin 2004 | 2004 |
| 5. Search for and identify evidence | Dimension | Ciardhuáin 2004 | 2004 |
| 6. Collection of evidence | Dimension | Ciardhuáin 2004 | 2004 |
| 7. Transport of evidence | Dimension | Ciardhuáin 2004 | 2004 |
| 8. Storage of evidence | Dimension | Ciardhuáin 2004 | 2004 |
| 9. Examination of evidence | Dimension | Ciardhuáin 2004 | 2004 |
| 10. Hypothesis | Dimension | Ciardhuáin 2004 | 2004 |
| 11. Presentation of hypothesis | Dimension | Ciardhuáin 2004 | 2004 |
| 12. Proof/Defense of hypothesis | Dimension | Ciardhuáin 2004 | 2004 |
| 13. Dissemination of information | Dimension | Ciardhuáin 2004 | 2004 |

| | | | |
|---|---|---|---|
| IDS | Factor | Ciardhuáin 2004 | 2004 |
| Having external investigators | Factor | Ciardhuáin 2004 | 2004 |
| Information flow and controls | Dimension | Ciardhuáin 2004 | 2004 |
| Influence of external policies, regulation and legislation on the policies of the investigating organisation | Factor | Ciardhuáin 2004 | 2004 |
| Link between external policies, regulation & legislation, and organisational policies to information controls | Factor | Ciardhuáin 2004 | 2004 |
| Cost | Dimension | Rowlingson 2004 | 2004 |
| 1. Where is data generated? | Factor | Rowlingson 2004 | 2004 |
| 2. What format is it in? | Factor | Rowlingson 2004 | 2004 |
| 3. For how long is it stored? | Factor | Rowlingson 2004 | 2004 |
| 4. How is data currently controlled, secured and managed? | Dimension | Rowlingson 2004 | 2004 |
| 5. Who has access to the data? | Factor | Rowlingson 2004 | 2004 |
| 6. How much data is produced? | Factor | Rowlingson 2004 | 2004 |
| 7. Is it archived? If so where and for how long? | Factor | Rowlingson 2004 | 2004 |
| 8. How much is reviewed? | Factor | Rowlingson 2004 | 2004 |
| 9. What additional evidence sources could be enabled? | Factor | Rowlingson 2004 | 2004 |
| 10. Who is responsible for this data? | Factor | Rowlingson 2004 | 2004 |
| 11. Who is the formal owner of the data? | Factor | Rowlingson 2004 | 2004 |
| 12. How could data be made available to an investigation? | Dimension | Rowlingson 2004 | 2004 |
| To what business processes does data relate? | Factor | Rowlingson 2004 | 2004 |
| Does data contain personal information? | Factor | Rowlingson 2004 | 2004 |
| Definition of business scenarios requiring digital evidence | Factor | Rowlingson 2004 | 2004 |
| Identification of sources and types of potential evidence | Factor | Rowlingson 2004 | 2004 |
| Identification of evidence collection requirements | Factor | Rowlingson 2004 | 2004 |
| Capability for securely gathering legally admissible evidence | Dimension | Rowlingson 2004 | 2004 |
| Establishment of policies for secure storage and handling of potential evidence | Dimension | Rowlingson 2004 | 2004 |
| Monitoring of incidents detection and deterrence systems | Dimension | Rowlingson 2004 | 2004 |
| Specify when escalation to formal investigation must be launched | Factor | Rowlingson 2004 | 2004 |
| Train personnel in incident awareness, roles and legal aspects of digital evidence process | Dimension | Rowlingson 2004 | 2004 |
| Document incident-based case for the incident and its impact | Factor | Rowlingson 2004 | 2004 |

|  |  |  |  |
|---|---|---|---|
| Ensure legal review to facilitate action in response to incident | Factor | Rowlingson 2004 | 2004 |
| Keeping business continuity (w/o interruption) | Factor | Rowlingson 2004 | 2004 |
| Benefit/cost proportionality | Dimension | Rowlingson 2004 | 2004 |
| Potential crimes and disputes | Factor | Rowlingson 2004 | 2004 |
| Legality of collection process | Factor | Rowlingson 2004 | 2004 |
| Evidence collection requirements | Dimension | Rowlingson 2004 | 2004 |
| Retention of information | Dimension | Rowlingson 2004 | 2004 |
| Planning of the response | Dimension | Rowlingson 2004 | 2004 |
| Training | Dimension | Rowlingson 2004 | 2004 |
| Acceleration of the investigation | Dimension | Rowlingson 2004 | 2004 |
| Prevention of anonymous activities | Factor | Rowlingson 2004 | 2004 |
| Legal | Dimension | Rowlingson 2004 | 2004 |
| Technical | Dimension | Rowlingson 2004 | 2004 |
| Non-technical | Dimension | Rowlingson 2004 | 2004 |
| Personnel and external organizations | Dimension | Rowlingson 2004 | 2004 |
| Understanding possible evidence sources, how to gather evidence legally and cost-effectively, when to escalate into a formal investigation, and how to put together a case involving law enforcement agencies. | Dimension | Rowlingson 2004 | 2004 |
| Need for privacy | Factor | Danielsson & Tjøstheim 2004 | 2004 |
| Maturity of information security posture | Factor | Danielsson & Tjøstheim 2004 | 2004 |
| Legal requirements and constraints on collection and preservation of potential digital evidence | Dimension | Danielsson & Tjøstheim 2004 | 2004 |
| A method for analyzing the organizations' need for digital evidence | Factor | Danielsson & Tjøstheim 2004 | 2004 |
| Identification and classification of potential digital evidence sources | Factor | Danielsson & Tjøstheim 2004 | 2004 |
| Enumeration of technologies and processes for utilizing these sources | Factor | Danielsson & Tjøstheim 2004 | 2004 |
| Guidelines for preserving digital evidence, processes, procedures, and suggestions to use technologies | Dimension | Danielsson & Tjøstheim 2004 | 2004 |
| Guidance on when and how to report incidents | Factor | Danielsson & Tjøstheim 2004 | 2004 |
| Organization's crime and dispute history | Factor | Danielsson & Tjøstheim 2004 | 2004 |
| The different crimes and disputes the organization is likely to be exposed to | Factor | Danielsson & Tjøstheim 2004 | 2004 |
| Assets and customers | Dimension | Danielsson & Tjøstheim 2004 | 2004 |
| Management support | Factor | Wolfe 2004 | 2004 |
| Forensic policies | Dimension | Wolfe 2004 | 2004 |
| Validity of capture process | Factor | Wolfe 2004 | 2004 |

| | | | |
|---|---|---|---|
| Chain of evidence | Dimension | Wolfe 2004 | 2004 |
| Computing knowledge of investigators | Factor | Wolfe 2004 | 2004 |
| Teaching System Administrators and Incident Handlers how to respond to an incident | Factor | Casey 2005 | 2005 |
| Training individuals who deal with network intrusions as both Incident Handlers and Forensic Examiners. | Factor | Casey 2005 | 2005 |
| Identify the firm's most valuable digital assets | Factor | Casey 2005 | 2005 |
| Develop a strategy to prepare the underlying systems from a forensic viewpoint | Dimension | Casey 2005 | 2005 |
| Internal monitoring of network activities | Factor | Casey 2005 | 2005 |
| Case management and incident tracking | Dimension | Casey 2005 | 2005 |
| Amount of information that Incident Handlers preserve on compromised systems | Factor | Casey 2005 | 2005 |
| Communicating information to law enforcement, ISPs, and other third parties | Factor | Casey 2005 | 2005 |
| Developing reputation of tracking back intruders | Factor | Casey 2005 | 2005 |
| DF accreditation of staff | Factor | Chen, Tsai, Chen & Yee 2005 | 2005 |
| Laboratory accreditation and auditing | Dimension | Chen, Tsai, Chen & Yee 2005 | 2005 |
| Follow regulations | Factor | Chen, Tsai, Chen & Yee 2005 | 2005 |
| A quality assurance system that covers quality policies, activities, procedures, documentation, and management. | Dimension | Chen, Tsai, Chen & Yee 2005 | 2005 |
| Procedures to control the quality of documents | Dimension | Chen, Tsai, Chen & Yee 2005 | 2005 |
| Accreditation of outsourcing laboratories | Factor | Chen, Tsai, Chen & Yee 2005 | 2005 |
| Monitoring of the forensics process | Factor | Chen, Tsai, Chen & Yee 2005 | 2005 |
| Archive Management | Dimension | Chen, Tsai, Chen & Yee 2005 | 2005 |
| Forensic knowledge of IT management | Dimension | Quinn 2005 | 2005 |
| Policies and procedures | Dimension | Quinn 2005 | 2005 |
| Training of IT staff | Factor | Quinn 2005 | 2005 |
| Assess risk considering vulnerabilities, threats, loss/exposure, etc.; | Factor | Beebe & Clark 2005 | 2005 |
| Develop an information retention plan (both pre/post-incident); | Factor | Beebe & Clark 2005 | 2005 |
| Develop an Incident Response Plan, including policies, procedures, personnel assignments, technical requirements | Factor | Beebe & Clark 2005 | 2005 |
| Develop technical capabilities (e.g. | Factor | Beebe & Clark 2005 | 2005 |

| | | | |
|---|---|---|---|
| response toolkits); | | | |
| Train personnel; | Factor | Beebe & Clark 2005 | 2005 |
| Prepare host and network devices; | Factor | Beebe & Clark 2005 | 2005 |
| Develop evidence preservation and handling procedures; and | Factor | Beebe & Clark 2005 | 2005 |
| Develop legal activities coordination plan (both pre/post-incident) | Factor | Beebe & Clark 2005 | 2005 |
| Timely short investigation process | Factor | Rogers, Goldman, Mislan, Wedge & Debrota 2006 | 2006 |
| 1. Find useable evidence immediately; | Factor | Rogers, Goldman, Mislan, Wedge & Debrota 2006 | 2006 |
| 2. Identify victims at acute risk; | Factor | Rogers, Goldman, Mislan, Wedge & Debrota 2006 | 2006 |
| 3. Guide the ongoing investigation; | Factor | Rogers, Goldman, Mislan, Wedge & Debrota 2006 | 2006 |
| 4. Identify potential charges; | Factor | Rogers, Goldman, Mislan, Wedge & Debrota 2006 | 2006 |
| 5. Accurately assess the offender’s danger to society | Factor | Rogers, Goldman, Mislan, Wedge & Debrota 2006 | 2006 |
| Does the warrant allow for the seizure and removal of the system(s)? | Factor | Rogers, Goldman, Mislan, Wedge & Debrota 2006 | 2006 |
| Is there sufficient particularity in the warrant and application for the warrant that allows for an onsite or in situ examination? | Factor | Rogers, Goldman, Mislan, Wedge & Debrota 2006 | 2006 |
| Are there any 4th Amendment issues that need to be addressed? | Factor | Rogers, Goldman, Mislan, Wedge & Debrota 2006 | 2006 |
| What are the reporting obligations to the issuing magistrate or judge? | Factor | Rogers, Goldman, Mislan, Wedge & Debrota 2006 | 2006 |
| Are there particular discovery issues present or anticipated? | Factor | Rogers, Goldman, Mislan, Wedge & Debrota 2006 | 2006 |
| Conducting an onsite examination affects the integrity of the original evidence? | Factor | Rogers, Goldman, Mislan, Wedge & Debrota 2006 | 2006 |
| The type of case? | Factor | Rogers, Goldman, Mislan, Wedge & Debrota 2006 | 2006 |
| How critical is the time factor? | Factor | Rogers, Goldman, Mislan, Wedge & Debrota 2006 | 2006 |
| What are the skills and abilities of the computer forensic examiners? | Dimension | Rogers, Goldman, Mislan, Wedge & Debrota 2006 | 2006 |
| What type of technology is involved (standalone systems, complex networks etc.)? | Dimension | Rogers, Goldman, Mislan, Wedge & Debrota 2006 | 2006 |
| Can the scene be safely and effectively controlled? | Factor | Rogers, Goldman, Mislan, Wedge & Debrota 2006 | 2006 |
| Can the systems in question be powered off or must they remain “live”? | Factor | Rogers, Goldman, Mislan, Wedge & Debrota 2006 | 2006 |
| What is the technical skill and knowledge level of the suspect? | Factor | Rogers, Goldman, Mislan, Wedge & Debrota 2006 | 2006 |
| Do the computer forensic examiners have the proper equipment for onsite examinations? | Factor | Rogers, Goldman, Mislan, Wedge & Debrota 2006 | 2006 |
| Maintaining the integrity of digital | Dimension | Rogers, Goldman, Mislan, | 2006 |

| | | | |
|---|---|---|---|
| evidence | | Wedge & Debrota 2006 | |
| Maintaining the chain of custody of evidence | Dimension | Rogers, Goldman, Mislan, Wedge & Debrota 2006 | 2006 |
| Complying with rules of evidence for admissibility at the Federal and State levels | Dimension | Rogers, Goldman, Mislan, Wedge & Debrota 2006 | 2006 |
| Planning and pre-raid intelligence | Dimension | Rogers, Goldman, Mislan, Wedge & Debrota 2006 | 2006 |
| Multiple physical and virtual locations, wired and wireless networks, and OS | Factor | Rogers, Goldman, Mislan, Wedge & Debrota 2006 | 2006 |
| Triaging the investigation (Rank in terms of importance or priority) | Factor | Rogers, Goldman, Mislan, Wedge & Debrota 2006 | 2006 |
| Toolkit (with hardware write blocker) | Factor | Rogers, Goldman, Mislan, Wedge & Debrota 2006 | 2006 |
| Profiling use/users/suspects (Home directory, File properties, Registry) | Factor | Rogers, Goldman, Mislan, Wedge & Debrota 2006 | 2006 |
| Define temporal value of evidence (MAC times, cookies, cache and the index.dat file) | Factor | Rogers, Goldman, Mislan, Wedge & Debrota 2006 | 2006 |
| Evaluate type of Internet activities (Cookies, Temps, URLs, Email, IM) | Factor | Rogers, Goldman, Mislan, Wedge & Debrota 2006 | 2006 |
| Focus on case specific evidence | Factor | Rogers, Goldman, Mislan, Wedge & Debrota 2006 | 2006 |
| Resistance through Firewalls | Factor | Endicott-Popovsky & Frincke 2006 | 2006 |
| Resistance through User authentication | Factor | Endicott-Popovsky & Frincke 2006 | 2006 |
| Resistance through Diversification | Factor | Endicott-Popovsky & Frincke 2006 | 2006 |
| Recognition through IDS | Factor | Endicott-Popovsky & Frincke 2006 | 2006 |
| Recognition through Internal Integrity Checks | Factor | Endicott-Popovsky & Frincke 2006 | 2006 |
| Recovery through Incident response | Factor | Endicott-Popovsky & Frincke 2006 | 2006 |
| Recovery through Replication | Factor | Endicott-Popovsky & Frincke 2006 | 2006 |
| Recovery through Backup systems | Factor | Endicott-Popovsky & Frincke 2006 | 2006 |
| Recovery through Fault tolerant designs | Factor | Endicott-Popovsky & Frincke 2006 | 2006 |
| Redress through computer forensics | Factor | Endicott-Popovsky & Frincke 2006 | 2006 |
| Redress by pursuing accountability for intruder behavior in the legal system | Factor | Endicott-Popovsky & Frincke 2006 | 2006 |
| Redress through active defense | Factor | Endicott-Popovsky & Frincke 2006 | 2006 |
| Policies including contacting law enforcement, performing monitoring, and<br>conducting regular reviews of forensic policies and procedures | Dimension | Kent, Chevalier, Grance & Dang 2006 | 2006 |
| Procedures and guidelines for performing forensic tasks,based on | Dimension | Kent, Chevalier, Grance & Dang 2006 | 2006 |

| | | | |
|---|---|---|---|
| the organization’s policies and all applicable laws and regulations | | | |
| Policies and procedures supporting reasonable and appropriate use of forensic tools | Dimension | Kent, Chevalier, Grance & Dang 2006 | 2006 |
| Legal advisors review of forensic policy and high-level procedures | Factor | Kent, Chevalier, Grance & Dang 2006 | 2006 |
| IT professionals prepared to participate in forensic activities | Factor | Kent, Chevalier, Grance & Dang 2006 | 2006 |
| Interactions between forensic staff and other teams | Factor | Kent, Chevalier, Grance & Dang 2006 | 2006 |
| Separation of policy for incident handlers and others with forensic roles | Factor | Kent, Chevalier, Grance & Dang 2006 | 2006 |
| Policies on roles and responsibilities of all people and external organizations | Factor | Kent, Chevalier, Grance & Dang 2006 | 2006 |
| The policy should discuss jurisdictional conflicts | Factor | Kent, Chevalier, Grance & Dang 2006 | 2006 |
| Providing Guidance for Forensic Tool Use | Factor | Kent, Chevalier, Grance & Dang 2006 | 2006 |
| Sensitive information safeguards and handling of inadvertent exposures | Factor | Kent, Chevalier, Grance & Dang 2006 | 2006 |
| Performing regular backups of systems and maintaining previous backups for a specific period of time | Factor | Kent, Chevalier, Grance & Dang 2006 | 2006 |
| Enabling auditing on workstations, servers, and network devices | Factor | Kent, Chevalier, Grance & Dang 2006 | 2006 |
| Forwarding audit records to secure centralized log servers | Factor | Kent, Chevalier, Grance & Dang 2006 | 2006 |
| Configuring mission-critical applications to perform auditing, including recording all authentication attempts | Factor | Kent, Chevalier, Grance & Dang 2006 | 2006 |
| Maintaining a DB of file hashes for the files of common OS and application deployments, and using file integrity checking software on important assets | Factor | Kent, Chevalier, Grance & Dang 2006 | 2006 |
| Maintaining records (e.g., baselines) of network and system configurations | Factor | Kent, Chevalier, Grance & Dang 2006 | 2006 |
| Establishing data retention policies for historical reviews of system and network activity | Factor | Kent, Chevalier, Grance & Dang 2006 | 2006 |
| Comply with requirements to preserve data on ongoing litigation and investigations | Factor | Kent, Chevalier, Grance & Dang 2006 | 2006 |
| Destroying data that is no longer needed | Factor | Kent, Chevalier, Grance & Dang 2006 | 2006 |
| Procedures for performing routine tasks (e.g. imaging a hard disk, capturing and recording volatile information from systems, or securing physical evidence | Factor | Kent, Chevalier, Grance & Dang 2006 | 2006 |
| Demonstrate conclusively the | Dimension | Kent, Chevalier, Grance & | 2006 |

| | | | |
|---|---|---|---|
| authenticity, credibility, and reliability of electronic records | | Dang 2006 | |
| Capability to perform computer and network forensics | Dimension | Kent, Chevalier, Grance & Dang 2006 | 2006 |
| Incident handling teams should have robust forensic capabilities | Factor | Kent, Chevalier, Grance & Dang 2006 | 2006 |
| Incorporating forensic considerations into the information system life cycle | Factor | Kent, Chevalier, Grance & Dang 2006 | 2006 |
| Centralized logging | Factor | Kent, Chevalier, Grance & Dang 2006 | 2006 |
| Security monitoring controls (e.g. IDS, antivirus software, and spyware detection and removal utilities) | Factor | Kent, Chevalier, Grance & Dang 2006 | 2006 |
| Monitoring of user behavior, such as keystroke monitoring | Factor | Kent, Chevalier, Grance & Dang 2006 | 2006 |
| Developing a plan to acquire the data, acquiring the data, and verifying the integrity of the acquired data. | Factor | Kent, Chevalier, Grance & Dang 2006 | 2006 |
| Detailed log and documentation of every step of data collection, including information about tools used | Factor | Kent, Chevalier, Grance & Dang 2006 | 2006 |
| Audience Consideration | Factor | Kent, Chevalier, Grance & Dang 2006 | 2006 |
| Consistency of processes | Factor | Kent, Chevalier, Grance & Dang 2006 | 2006 |
| Awareness of data sources | Factor | Kent, Chevalier, Grance & Dang 2006 | 2006 |
| Proactive collection of data | Factor | Kent, Chevalier, Grance & Dang 2006 | 2006 |
| Procedure for collecting volatile data | Factor | Kent, Chevalier, Grance & Dang 2006 | 2006 |
| Attacker Identification | Factor | Kent, Chevalier, Grance & Dang 2006 | 2006 |
| 1. What are the potential sources of data? | Dimension | Kent, Chevalier, Grance & Dang 2006 | 2006 |
| 2. Of the potential sources of data, which are the most likely to contain helpful information and why? | Factor | Kent, Chevalier, Grance & Dang 2006 | 2006 |
| 3. Which data source would be checked first and why? | Factor | Kent, Chevalier, Grance & Dang 2006 | 2006 |
| 4. Which forensic tools and techniques would most likely be used? Which other tools and techniques might also be used? | Dimension | Kent, Chevalier, Grance & Dang 2006 | 2006 |
| 5. Which groups and individuals within the organization would probably be involved in the forensic activities? | Dimension | Kent, Chevalier, Grance & Dang 2006 | 2006 |
| 6. What communications with external parties might occur, if any? | Dimension | Kent, Chevalier, Grance & Dang 2006 | 2006 |
| 7. From a forensic standpoint, what would be done differently if the scenario had occurred on a different day or at a different time (regular | Factor | Kent, Chevalier, Grance & Dang 2006 | 2006 |

| | | | |
|---|---|---|---|
| hours versus off-hours)? | | | |
| 8. From a forensic standpoint, what would be done differently if the scenario had occurred at a different physical location (onsite versus offsite)? | Factor | Kent, Chevalier, Grance & Dang 2006 | 2006 |
| The existence of a toolkit | Factor | Kent, Chevalier, Grance & Dang 2006 | 2006 |
| The existence of a response team | Factor | Kent, Chevalier, Grance & Dang 2006 | 2006 |
| Clear weighed criteria on whether turning off a hacked device | Factor | Kent, Chevalier, Grance & Dang 2006 | 2006 |
| Clear weighed criteria on volatility orders to collect evidence in each case | Factor | Kent, Chevalier, Grance & Dang 2006 | 2006 |
| Information Management Team including experts in computer forensics, law, information management, information technology, and auditing | Dimension | Luoma 2006 | 2006 |
| Electronic document retention and deletion policy | Dimension | Luoma 2006 | 2006 |
| Fexibility to implement litigation holds by suspending routine document deletion when litigation is imminent | Factor | Luoma 2006 | 2006 |
| Determination of what documents should be retained and when they should be destroyed | Factor | Luoma 2006 | 2006 |
| Management support for the forensic team | Factor | Luoma 2006 | 2006 |
| Information Management Director distinct from the Information Systems/Technology Director | Factor | Luoma 2006 | 2006 |
| Employees knowledge on information management and awareness of policies | Dimension | Luoma 2006 | 2006 |
| Regular information management audit | Factor | Luoma 2006 | 2006 |
| Determining sources of electronic data being used by the organization's employees | Factor | Luoma 2006 | 2006 |
| Information Security Governance thorugh top management commitment | Factor | VonSolms 2006 | 2006 |
| Information Security Governance thorugh organizational structures | Factor | VonSolms 2006 | 2006 |
| Information Security Governance thorugh user awareness and commitment | Factor | VonSolms 2006 | 2006 |
| Information Security Governance thorugh technology, policies, procedures and enforcement | Factor | VonSolms 2006 | 2006 |
| Planning Information Retention Requirements | Dimension | VonSolms, Lowurens, Reeky & Grobler 2006 | 2006 |

| | | | |
|---|---|---|---|
| Define the business scenarios that require digital evidence | Factor | VonSolms, Lowurens, Reeky & Grobler 2006 | 2006 |
| Identify available sources and different types of potential evidence | Factor | VonSolms, Lowurens, Reeky & Grobler 2006 | 2006 |
| Determine the evidence collection requirement | Factor | VonSolms, Lowurens, Reeky & Grobler 2006 | 2006 |
| Establish policy for secure storage and handling of potential evidence | Factor | VonSolms, Lowurens, Reeky & Grobler 2006 | 2006 |
| Establish a capability for securely gathering legally admissible evidence to meet the requirement | Factor | VonSolms, Lowurens, Reeky & Grobler 2006 | 2006 |
| Synchronize all relevant devices and systems | Factor | VonSolms, Lowurens, Reeky & Grobler 2006 | 2006 |
| Gather potential evidence | Dimension | VonSolms, Lowurens, Reeky & Grobler 2006 | 2006 |
| Prevent anonymous activities | Dimension | VonSolms, Lowurens, Reeky & Grobler 2006 | 2006 |
| Planning the response. | Dimension | VonSolms, Lowurens, Reeky & Grobler 2006 | 2006 |
| Ensure monitoring is targeted to detect and deter major incidents | Factor | VonSolms, Lowurens, Reeky & Grobler 2006 | 2006 |
| Implement IDS | Factor | VonSolms, Lowurens, Reeky & Grobler 2006 | 2006 |
| Specify circumstances when escalation to a full formal investigation should be launched | Factor | VonSolms, Lowurens, Reeky & Grobler 2006 | 2006 |
| Establish a Computer Emergency Response Team (CERT) | Factor | VonSolms, Lowurens, Reeky & Grobler 2006 | 2006 |
| Establish capabilities and response times for external digital forensic investigation professionals | Factor | VonSolms, Lowurens, Reeky & Grobler 2006 | 2006 |
| Digital Forensic Training | Dimension | VonSolms, Lowurens, Reeky & Grobler 2006 | 2006 |
| Train staff in incident awareness to understand roles and sensitivity of evidence | Factor | VonSolms, Lowurens, Reeky & Grobler 2006 | 2006 |
| Develop an in-house investigative capability if required | Factor | VonSolms, Lowurens, Reeky & Grobler 2006 | 2006 |
| Enhance capability for evidence retrieval | Factor | VonSolms, Lowurens, Reeky & Grobler 2006 | 2006 |
| Accelerating the DF investigation. | Dimension | VonSolms, Lowurens, Reeky & Grobler 2006 | 2006 |
| Document and validate an investigation protocol against best practice | Factor | VonSolms, Lowurens, Reeky & Grobler 2006 | 2006 |
| Acquire appropriate DF tools and systems | Factor | VonSolms, Lowurens, Reeky & Grobler 2006 | 2006 |
| Ensure legal review to facilitate action in response to the incident | Factor | VonSolms, Lowurens, Reeky & Grobler 2006 | 2006 |
| Define responsibilities and authority for CERT and investigative teams | Factor | VonSolms, Lowurens, Reeky & Grobler 2006 | 2006 |
| Define circumstances for engaging professional investigative services | Factor | VonSolms, Lowurens, Reeky & Grobler 2006 | 2006 |
| Speed of reaction | Factor | Forrester & Irwin 2007 | 2007 |
| Review of previous incidents | Factor | Forrester & Irwin 2007 | 2007 |

| | | | |
|---|---|---|---|
| Incident response team | Dimension | Forrester & Irwin 2007 | 2007 |
| Organisational policies and procedures | Dimension | Forrester & Irwin 2007 | 2007 |
| Pre-emptive systems in place | Dimension | Forrester & Irwin 2007 | 2007 |
| Corporate governance material converted into a Forensic Readiness Policy | Dimension | Forrester & Irwin 2007 | 2007 |
| Legal context | Dimension | Forrester & Irwin 2007 | 2007 |
| Management conviction of the importance of DFR | Factor | Grobler & Louwrens 2007 | 2007 |
| Good corporate governance, specifically IS governance | Dimension | Grobler & Louwrens 2007 | 2007 |
| To enrich / augment the security program of the organization so adequate evidence, processes and procedures are in place to determine the source of an attack | Factor | Grobler & Louwrens 2007 | 2007 |
| Use of DF tools | Dimension | Grobler & Louwrens 2007 | 2007 |
| To prevent the use of anti-forensic strategies for example data destruction or manipulation and data hiding | Factor | Grobler & Louwrens 2007 | 2007 |
| IS and DF awareness training | Dimension | Grobler & Louwrens 2007 | 2007 |
| IS and DF policies | Dimension | Grobler & Louwrens 2007 | 2007 |
| Identifying all the business scenarios that will require digital evidence | Factor | Grobler & Louwrens 2007 | 2007 |
| Determine the vulnerabilities and threats and what evidence will be required to determine the rootcause of the event | Factor | Grobler & Louwrens 2007 | 2007 |
| Determine what information is required for evidence (the format and exactly what is required) | Factor | Grobler & Louwrens 2007 | 2007 |
| Determine how to legally capture and preserve the evidence considering privacy | Factor | Grobler & Louwrens 2007 | 2007 |
| Ensure that monitoring is targeted to detect and deter incidents; | Factor | Grobler & Louwrens 2007 | 2007 |
| Augment the IRP to specify when to escalate to a full investigation; | Factor | Grobler & Louwrens 2007 | 2007 |
| Define the first response guidelines to the Incident response plan to preserve evidence | Factor | Grobler & Louwrens 2007 | 2007 |
| Determine when and how to activate Disaster recovery plan (DRP) and Business Continuity plan (BCP) | Factor | Grobler & Louwrens 2007 | 2007 |
| Establish an organizational structure with roles and responsibilities to deal with DF in the organization with segregation of DF and IS teams duties | Factor | Grobler & Louwrens 2007 | 2007 |
| Establish a digital evidence management program | Factor | Grobler & Louwrens 2007 | 2007 |
| Incorporate DF techniques in the IS | Factor | Grobler & Louwrens 2007 | 2007 |

|  |  |  |  |
|---|---|---|---|
| auditing procedures |  |  |  |
| Access controls should be reviewed to prevent anonymous activities; | Factor | Grobler & Louwrens 2007 | 2007 |
| Establish a capability to securely gather admissible evidence by considering technology and human capacity | Dimension | Grobler & Louwrens 2007 | 2007 |
| Use DF tools and processes to demonstrate good corporate governance | Factor | Grobler & Louwrens 2007 | 2007 |
| Use DF tools for non-forensic purposes to enhance the ISA, for example data recovery if a hard disk crashes | Factor | Grobler & Louwrens 2007 | 2007 |
| Developing a preservation culture in the organization to preserve all processes and activities should an investigation arise; | Dimension | Grobler & Louwrens 2007 | 2007 |
| Design all security controls to prevent any anti-forensic activities (No password crackers, key-loggers, steganography software etc.) | Factor | Grobler & Louwrens 2007 | 2007 |
| Monitoring and controlling removable / portable devices | Factor | Grobler & Louwrens 2007 | 2007 |
| Accepting an expanded role for systems and network administrators | Factor | Endicott-Popovsky, Frincke & Taylor 2007 | 2007 |
| Understanding of how legal requirements for admissible evidence can be translated into information system requirements | Factor | Endicott-Popovsky, Frincke & Taylor 2007 | 2007 |
| Embedding forensic capabilities in networks | Factor | Endicott-Popovsky, Frincke & Taylor 2007 | 2007 |
| Ability to repel attacks using tools such as Firewalls, User authentication, and Diversification. | Factor | Endicott-Popovsky, Frincke & Taylor 2007 | 2007 |
| Ability to detect an attack or a probe using IDS, and Internal integrity checks. | Factor | Endicott-Popovsky, Frincke & Taylor 2007 | 2007 |
| Ability to provide essential services during attack and restore services using Incident response, Replication, Backup systems, and Fault tolerant design. | Factor | Endicott-Popovsky, Frincke & Taylor 2007 | 2007 |
| Ability to hold intruders accountable in a court of law and to retaliate using Forensics (the who), legal remedies and active defense. | Factor | Endicott-Popovsky, Frincke & Taylor 2007 | 2007 |
| The identification of relevant target assets. | Factor | Endicott-Popovsky, Frincke & Taylor 2007 | 2007 |
| The test and calibration of the collection devices and their frequency of calibration | Factor | Endicott-Popovsky, Frincke & Taylor 2007 | 2007 |
| Including DF into the ISDLC | Factor | Endicott-Popovsky, Frincke & Taylor 2007 | 2007 |
| Identification of assets of value | Factor | Taylor, Endicott-Popovsky & Frincke 2007 | 2007 |

| | | | |
|---|---|---|---|
| Performance of risk assessment for potential losses and threats | Factor | Taylor, Endicott-Popovsky & Frincke 2007 | 2007 |
| Removal of assets that do not warrant the effort of prosecution | Factor | Taylor, Endicott-Popovsky & Frincke 2007 | 2007 |
| Identification of associated data linked to valuable assets | Factor | Taylor, Endicott-Popovsky & Frincke 2007 | 2007 |
| Identification of collection and storage needs for data | Factor | Taylor, Endicott-Popovsky & Frincke 2007 | 2007 |
| Establishment of policies in terms of digital assets, forensic events, data collection and storage | Dimension | Taylor, Endicott-Popovsky & Frincke 2007 | 2007 |
| Forensics policy enforcement | Factor | Taylor, Endicott-Popovsky & Frincke 2007 | 2007 |
| Is the evidence based on a testable theory or technique? | Factor | Bem, Feld, Huebner & Bem 2008 | 2008 |
| In the case of a particular technique, does it have a known or potential error rate? | Factor | Bem, Feld, Huebner & Bem 2008 | 2008 |
| Does the technique have and maintain standards controlling its operation? | Factor | Bem, Feld, Huebner & Bem 2008 | 2008 |
| Is the underlying science generally accepted within the relevant scientific community? | Factor | Bem, Feld, Huebner & Bem 2008 | 2008 |
| Has the theory or technique been subjected to peer review? | Factor | Bem, Feld, Huebner & Bem 2008 | 2008 |
| Lack of Standards within the Discipline | Factor | Bem, Feld, Huebner & Bem 2008 | 2008 |
| Storage capacity | Factor | Bem, Feld, Huebner & Bem 2008 | 2008 |
| File and operating systems | Factor | Bem, Feld, Huebner & Bem 2008 | 2008 |
| Online storage | Factor | Bem, Feld, Huebner & Bem 2008 | 2008 |
| Storage visualization abilities | Factor | Bem, Feld, Huebner & Bem 2008 | 2008 |
| Decryption ability | Factor | Bem, Feld, Huebner & Bem 2008 | 2008 |
| Small and easy to hide storage devices | Factor | Bem, Feld, Huebner & Bem 2008 | 2008 |
| Volatility | Factor | Bem, Feld, Huebner & Bem 2008 | 2008 |
| A triage process model of analysis and interpretation of digital evidence | Factor | Bem, Feld, Huebner & Bem 2008 | 2008 |
| Ability to recreate the investigated environment | Factor | Bem, Feld, Huebner & Bem 2008 | 2008 |
| Multidisciplinary approach (Law, IT, Enforcement, Business) | Dimension | Bem, Feld, Huebner & Bem 2008 | 2008 |
| Computer Security Incident Response Teams (CSIRTs) | Dimension | Khurana, Basney, Bakht, Freemon, Welch & Butler 2009 | 2009 |
| Digital investigation procedures | Dimension | Khurana, Basney, Bakht, Freemon, Welch & Butler 2009 | 2009 |
| Sharing of logs across institutional boundaries | Factor | Khurana, Basney, Bakht, Freemon, Welch & Butler 2009 | 2009 |
| Interaction with law enforcement | Dimension | Khurana, Basney, Bakht, Freemon, Welch & Butler 2009 | 2009 |

|  |  |  |  |
|---|---|---|---|
| Interaction with the media | Factor | Khurana, Basney, Bakht, Freemon, Welch & Butler 2009 | 2009 |
| Independent Center for Incident Management (ICIM) | Factor | Khurana, Basney, Bakht, Freemon, Welch & Butler 2009 | 2009 |
| Collectively define access policies | Factor | Khurana, Basney, Bakht, Freemon, Welch & Butler 2009 | 2009 |
| Role based access control with the least privilege principle in mind | Factor | Khurana, Basney, Bakht, Freemon, Welch & Butler 2009 | 2009 |
| Emergency Response Teams (CERTs) | Dimension | Khurana, Basney, Bakht, Freemon, Welch & Butler 2009 | 2009 |
| Establish adequate levels of trust between the involved institutions and personnel | Factor | Khurana, Basney, Bakht, Freemon, Welch & Butler 2009 | 2009 |
| Managing all the tasks and processes in the response and investigation processes | Factor | Khurana, Basney, Bakht, Freemon, Welch & Butler 2009 | 2009 |
| Analysis of logs and alerts gathered by IDSs, server logs, and network logs | Dimension | Khurana, Basney, Bakht, Freemon, Welch & Butler 2009 | 2009 |
| Roles and Responsibilities Model | Dimension | Khurana, Basney, Bakht, Freemon, Welch & Butler 2009 | 2009 |
| Process Model defining the phases of the response and investigation process | Factor | Khurana, Basney, Bakht, Freemon, Welch & Butler 2009 | 2009 |
| Strong two-factor authentication | Factor | Khurana, Basney, Bakht, Freemon, Welch & Butler 2009 | 2009 |
| Secured network perimeter around the servers of a centralized workspace | Factor | Khurana, Basney, Bakht, Freemon, Welch & Butler 2009 | 2009 |
| Plethora of useful tools (IDS, Centralized logging) | Dimension | Khurana, Basney, Bakht, Freemon, Welch & Butler 2009 | 2009 |
| Distinguish between site roles and collaboration roles | Factor | Khurana, Basney, Bakht, Freemon, Welch & Butler 2009 | 2009 |
| Site Technical Roles (Lead, Incident Investigator, Digital Forensics Specialist, Security/System Administrator, Security/System Architect) | Dimension | Khurana, Basney, Bakht, Freemon, Welch & Butler 2009 | 2009 |
| Collaboration Technical Roles (Lead, Incident Investigator, Digital Forensics Specialist, Workspace Administrator) | Dimension | Khurana, Basney, Bakht, Freemon, Welch & Butler 2009 | 2009 |
| Site Legal Roles (Legal Adviser, Liason with Law Enforcement) | Dimension | Khurana, Basney, Bakht, Freemon, Welch & Butler 2009 | 2009 |
| Law Enforcement Roles (Prosecutor, Investigator, Executive, Media Liason) | Dimension | Khurana, Basney, Bakht, Freemon, Welch & Butler 2009 | 2009 |
| Preparation of security system architecture documentation | Dimension | Khurana, Basney, Bakht, Freemon, Welch & Butler 2009 | 2009 |
| Train staff on latest threats and software tools | Dimension | Khurana, Basney, Bakht, Freemon, Welch & Butler 2009 | 2009 |
| Follow recommended practices to prevent incidents | Factor | Khurana, Basney, Bakht, Freemon, Welch & Butler 2009 | 2009 |
| Deploy intrusion detection and forensics data collection capabilities | Dimension | Khurana, Basney, Bakht, Freemon, Welch & Butler 2009 | 2009 |
| Develop incident response policies, | Dimension | Khurana, Basney, Bakht, | 2009 |

| | | | |
|---|---|---|---|
| procedures and legal coordination plan | | Freemon, Welch & Butler 2009 | |
| Establish and maintain a collaborative workspace hosting environment | Dimension | Khurana, Basney, Bakht, Freemon, Welch & Butler 2009 | 2009 |
| Develop/deploy collaborative tools, policies and procedures | Dimension | Khurana, Basney, Bakht, Freemon, Welch & Butler 2009 | 2009 |
| Chain of custody | Dimension | Khurana, Basney, Bakht, Freemon, Welch & Butler 2009 | 2009 |
| Identify the lessons that can be learned from the handling of the incident | Factor | Khurana, Basney, Bakht, Freemon, Welch & Butler 2009 | 2009 |
| Wizards in the workspace environment | Factor | Khurana, Basney, Bakht, Freemon, Welch & Butler 2009 | 2009 |
| Information Sharing and Analysis Centers (ISACs) | Factor | Khurana, Basney, Bakht, Freemon, Welch & Butler 2009 | 2009 |
| Multi-user systems | Factor | Dlamini, Eloff, & Eloff 2009 | 2009 |
| Digital signatures | Factor | Dlamini, Eloff, & Eloff 2009 | 2009 |
| Encryption standards | Factor | Dlamini, Eloff, & Eloff 2009 | 2009 |
| Anti virus software environments and filtering firewalls | Factor | Dlamini, Eloff, & Eloff 2009 | 2009 |
| Authorization and authentication credentials | Factor | Dlamini, Eloff, & Eloff 2009 | 2009 |
| ID Management | Dimension | Dlamini, Eloff, & Eloff 2009 | 2009 |
| Information Security Awareness | Factor | Dlamini, Eloff, & Eloff 2009 | 2009 |
| Information Security Management | Dimension | Dlamini, Eloff, & Eloff 2009 | 2009 |
| Legal & Regulatory Compliance | Dimension | Dlamini, Eloff, & Eloff 2009 | 2009 |
| Network Security | Dimension | Dlamini, Eloff, & Eloff 2009 | 2009 |
| Perimeter Security | Factor | Dlamini, Eloff, & Eloff 2009 | 2009 |
| Physical Security | Dimension | Dlamini, Eloff, & Eloff 2009 | 2009 |
| Privacy | Dimension | Dlamini, Eloff, & Eloff 2009 | 2009 |
| Risk Management | Dimension | Dlamini, Eloff, & Eloff 2009 | 2009 |
| Software Security | Dimension | Dlamini, Eloff, & Eloff 2009 | 2009 |
| Standardization, configuration management | Factor | Dlamini, Eloff, & Eloff 2009 | 2009 |
| PKI implementation | Factor | Dlamini, Eloff, & Eloff 2009 | 2009 |
| Endpoint security | Factor | Dlamini, Eloff, & Eloff 2009 | 2009 |
| Managed cybersecurity provider | Factor | Dlamini, Eloff, & Eloff 2009 | 2009 |
| Two-factor authentication | Factor | Dlamini, Eloff, & Eloff 2009 | 2009 |
| Employee misuse | Factor | Dlamini, Eloff, & Eloff 2009 | 2009 |
| Intrusion detection systems | Factor | Dlamini, Eloff, & Eloff 2009 | 2009 |
| Patch management | Factor | Dlamini, Eloff, & Eloff 2009 | 2009 |
| Wireless infrastructure security | Dimension | Dlamini, Eloff, & Eloff 2009 | 2009 |
| Internal network security | Dimension | Dlamini, Eloff, & Eloff 2009 | 2009 |
| Access control | Factor | Dlamini, Eloff, & Eloff 2009 | 2009 |
| Management involvement, risk management | Dimension | Dlamini, Eloff, & Eloff 2009 | 2009 |
| User education, training and awareness | Dimension | Dlamini, Eloff, & Eloff 2009 | 2009 |

| | | | |
|---|---|---|---|
| Policy & regulatory compliance (Sarbanes–Oxley, HIPAA) | Dimension | Dlamini, Eloff, & Eloff 2009 | 2009 |
| Data protection | Dimension | Dlamini, Eloff, & Eloff 2009 | 2009 |
| An overall forensic policy | Dimension | Reddy & Venter 2009 | 2009 |
| Technical readiness procedures and processes | Dimension | Reddy & Venter 2009 | 2009 |
| Non-technical readiness procedures and processes | Dimension | Reddy & Venter 2009 | 2009 |
| Monitoring and auditing | Dimension | Reddy & Venter 2009 | 2009 |
| Hardware and software configured properly | Dimension | Reddy & Venter 2009 | 2009 |
| Education of forensic team members and appropriate certifications | Dimension | Reddy & Venter 2009 | 2009 |
| Multi-disciplinary team | Factor | Reddy & Venter 2009 | 2009 |
| Architecture | Dimension | Reddy & Venter 2009 | 2009 |
| Alignment of privacy policy with business policies | Factor | Reddy & Venter 2009 | 2009 |
| Virtualization | Factor | Garfinkel 2010 | 2010 |
| Size of storage | Factor | Garfinkel 2010 | 2010 |
| Variety of storage device | Factor | Garfinkel 2010 | 2010 |
| OS and File formats | Factor | Garfinkel 2010 | 2010 |
| Cost of tools | Factor | Garfinkel 2010 | 2010 |
| Pervasive encryption | Factor | Garfinkel 2010 | 2010 |
| Cloudification | Factor | Garfinkel 2010 | 2010 |
| Legal limitations | Dimension | Garfinkel 2010 | 2010 |
| Mobile computing | Dimension | Garfinkel 2010 | 2010 |
| Training | Dimension | Garfinkel 2010 | 2010 |
| International laws | Dimension | Garfinkel 2010 | 2010 |
| Functionality of DF tools | Dimension | Garfinkel 2010 | 2010 |
| Lack of standardization and automation in DF processes | Factor | Garfinkel 2010 | 2010 |
| Poor transfer of academic research to practice | Factor | Garfinkel 2010 | 2010 |
| Collaboration | Dimension | Garfinkel 2010 | 2010 |
| Strategy | Dimension | Barske, Stander & Jordaan 2010 | 2010 |
| Compliance & Monitoring | Dimension | Barske, Stander & Jordaan 2010 | 2010 |
| Policy & Procedures | Dimension | Barske, Stander & Jordaan 2010 | 2010 |
| Technology | Dimension | Barske, Stander & Jordaan 2010 | 2010 |
| Digital Forensic Response | Dimension | Barske, Stander & Jordaan 2010 | 2010 |
| Perception of high cost of forensics | Factor | Barske, Stander & Jordaan 2010 | 2010 |
| Lack of forensic skills | Factor | Barske, Stander & Jordaan 2010 | 2010 |
| Organization size | Factor | Barske, Stander & Jordaan 2010 | 2010 |

| | | | |
|---|---|---|---|
| Industry sector | Factor | Barske, Stander & Jordaan 2010 | 2010 |
| Available funding | Factor | Barske, Stander & Jordaan 2010 | 2010 |
| Number of employees | Factor | Barske, Stander & Jordaan 2010 | 2010 |
| Employees accessibility to financial instruments | Factor | Barske, Stander & Jordaan 2010 | 2010 |
| Staff IT skills | Dimension | Barske, Stander & Jordaan 2010 | 2010 |
| Public profile condition | Factor | Barske, Stander & Jordaan 2010 | 2010 |
| Proper legal authority to conduct the search and examination | Factor | Barske, Stander & Jordaan 2010 | 2010 |
| Chain of custody is kept for the evidence | Dimension | Barske, Stander & Jordaan 2010 | 2010 |
| Using forensic tools that have been validated | Factor | Barske, Stander & Jordaan 2010 | 2010 |
| The use of imaging and hashing functions to acquire evidence | Factor | Barske, Stander & Jordaan 2010 | 2010 |
| Quality assurance to ensure that the examination and analysis | Dimension | Barske, Stander & Jordaan 2010 | 2010 |
| ICT systems configuration | Factor | Barske, Stander & Jordaan 2010 | 2010 |
| Policy, people and process adaptation to DF | Dimension | Barske, Stander & Jordaan 2010 | 2010 |
| Updating the organisation's policies and procedures | Dimension | Barske, Stander & Jordaan 2010 | 2010 |
| Improvements in training of employees | Factor | Barske, Stander & Jordaan 2010 | 2010 |
| The systematic gathering of potential digital evidence | Dimension | Barske, Stander & Jordaan 2010 | 2010 |
| The secure storage of potential digital evidence | Dimension | Barske, Stander & Jordaan 2010 | 2010 |
| Preparation for events requiring digital forensic intervention | Dimension | Barske, Stander & Jordaan 2010 | 2010 |
| Enhanced capability for evidence retrieval | Dimension | Barske, Stander & Jordaan 2010 | 2010 |
| Legal advice | Dimension | Barske, Stander & Jordaan 2010 | 2010 |
| Developing of an in-house digital forensics examination and analysis capacity | Dimension | Barske, Stander & Jordaan 2010 | 2010 |
| Identifying and understanding retention records legislation | Dimension | Barske, Stander & Jordaan 2010 | 2010 |
| Determining which scenarios could potentially require digital evidence | Factor | Barske, Stander & Jordaan 2010 | 2010 |
| Identifying the available sources and different types of digital evidence | Factor | Barske, Stander & Jordaan 2010 | 2010 |
| Identifying policies needed to ensure DFR and legality of the DFR practices | Factor | Barske, Stander & Jordaan 2010 | 2010 |
| Identify the technological and human resources needed for DFR | Factor | Barske, Stander & Jordaan 2010 | 2010 |
| Ensure sufficient funding the set up and maintain the DFR program | Factor | Barske, Stander & Jordaan 2010 | 2010 |

| | | | |
|---|---|---|---|
| A policy for the acceptable use of information systems resources by members of the organization | Factor | Barske, Stander & Jordaan 2010 | 2010 |
| A policy clarifying organization ownership of information systems resources and data w/o expectation of privacy or ownership by employees, plus consent of monitoring | Factor | Barske, Stander & Jordaan 2010 | 2010 |
| A policy about information systems monitoring | Factor | Barske, Stander & Jordaan 2010 | 2010 |
| A policy which states what information and under what circumstances is preserved | Factor | Barske, Stander & Jordaan 2010 | 2010 |
| A policy which states the periods of time and categories of digital evidence retention, as well as the storage and secure handling thereof | Factor | Barske, Stander & Jordaan 2010 | 2010 |
| A policy which states the circumstance when internal investigations can be initiated and the actions that may be taken | Factor | Barske, Stander & Jordaan 2010 | 2010 |
| A policy which states the manner and circumstances of evidence release to external parties | Factor | Barske, Stander & Jordaan 2010 | 2010 |
| A policy for the roles and responsibilities of parties involved in preserving, maintaining and examining evidence | Factor | Barske, Stander & Jordaan 2010 | 2010 |
| A policy which stipulate a legal review process for any digital forensic investigation or incident | Factor | Barske, Stander & Jordaan 2010 | 2010 |
| Logs | Factor | Barske, Stander & Jordaan 2010 | 2010 |
| Computers and Servers | Dimension | Barske, Stander & Jordaan 2010 | 2010 |
| Acquisition and Analysis technology | Dimension | Barske, Stander & Jordaan 2010 | 2010 |
| Evidence Storage technology | Dimension | Barske, Stander & Jordaan 2010 | 2010 |
| Interdisciplinary formal programs to educate professionals | Dimension | Duranti & Endicott-Popovsky 2010 | 2010 |
| Infrastructure preparedness | Dimension | Grobler, Louwrens & Von Solms 2010 | 2010 |
| Development of evidence management plan (EMP) | Factor | Grobler, Louwrens & Von Solms 2010 | 2010 |
| Development of evidence map | Factor | Grobler, Louwrens & Von Solms 2010 | 2010 |
| Development of evidence management policies | Factor | Grobler, Louwrens & Von Solms 2010 | 2010 |
| Development of procedures to manage CDE | Factor | Grobler, Louwrens & Von Solms 2010 | 2010 |
| Existance of risk mitigation plans including evidence and process requirements | Dimension | Grobler, Louwrens & Von Solms 2010 | 2010 |
| Application of an algorithm to | Factor | Grobler, Louwrens & Von | 2010 |

| | | | |
|---|---|---|---|
| calculate completeness and admissibility of the evidence | | Solms 2010 | |
| Implementation of an Intrusion Detection System (IDS) | Factor | Grobler, Louwrens & Von Solms 2010 | 2010 |
| Definition of trigger events for investigations | Factor | Grobler, Louwrens & Von Solms 2010 | 2010 |
| Preparation for containments of incidents to include containment on live systems | Dimension | Grobler, Louwrens & Von Solms 2010 | 2010 |
| Development of a DF awareness program | Factor | Grobler, Louwrens & Von Solms 2010 | 2010 |
| Development of a DF training program | Factor | Grobler, Louwrens & Von Solms 2010 | 2010 |
| Development of a management capability for DF investigators and CERT | Factor | Grobler, Louwrens & Von Solms 2010 | 2010 |
| Documentation and validation of a DF investigation (DFI) protocol against best practice | Factor | Grobler, Louwrens & Von Solms 2010 | 2010 |
| Effectiveness of controls against IT and IS objectives | Factor | Grobler, Louwrens & Von Solms 2010 | 2010 |
| Use of IT tools | Dimension | Grobler, Louwrens & Von Solms 2010 | 2010 |
| Controls for the responsible use of DF tools | Factor | Grobler, Louwrens & Von Solms 2010 | 2010 |
| Existence of Computer Emergency Response Team (CERT) | Factor | Grobler, Louwrens & Von Solms 2010 | 2010 |
| Minimization of business interruption | Dimension | Grobler, Louwrens & Von Solms 2010 | 2010 |
| Effectiveness of controls | Factor | Grobler, Louwrens & Von Solms 2010 | 2010 |
| IT & IS Objectives vs business objectives | Factor | Grobler, Louwrens & Von Solms 2010 | 2010 |
| Efficiency | Dimension | Grobler, Louwrens & Von Solms 2010 | 2010 |
| Responsible use of DF tools | Factor | Grobler, Louwrens & Von Solms 2010 | 2010 |
| Specific requirements per country, jurisdiction, and industry for admissible evidence | Dimension | Grobler, Louwrens & Von Solms 2010 | 2010 |
| Ability to prove compliance | Dimension | Grobler, Louwrens & Von Solms 2010 | 2010 |
| Active DF capabilities in live system environments | Dimension | Grobler, Louwrens & Von Solms 2010 | 2010 |
| Pre-defined trigger event or procedures to start active monitoring | Factor | Grobler, Louwrens & Von Solms 2010 | 2010 |
| Soundness of processes | Factor | Grobler, Louwrens & Von Solms 2010 | 2010 |
| Education level of investigators and staff | Factor | Grobler, Louwrens & Von Solms 2010 | 2010 |
| Availability of acceptable tools and technologies | Factor | Grobler, Louwrens & Von Solms 2010 | 2010 |
| Establishment of policies and procedures | Dimension | Grobler, Louwrens & Von Solms 2010 (2) | 2010 |
| Legal | Dimension | Grobler, Louwrens & Von Solms 2010 (2) | 2010 |

| | | | |
|---|---|---|---|
| Policies | Dimension | Grobler, Louwrens & Von Solms 2010 (2) | 2010 |
| Governance | Dimension | Grobler, Louwrens & Von Solms 2010 (2) | 2010 |
| People | Dimension | Grobler, Louwrens & Von Solms 2010 (2) | 2010 |
| Process | Dimension | Grobler, Louwrens & Von Solms 2010 (2) | 2010 |
| Technology | Dimension | Grobler, Louwrens & Von Solms 2010 (2) | 2010 |
| The digital media in question | Factor | Hoolachan & Glisson 2010 | 2010 |
| Implemented processes and methodologies | Dimension | Hoolachan & Glisson 2010 | 2010 |
| Legal aspects | Dimension | Hoolachan & Glisson 2010 | 2010 |
| The individuals involved in the investigation | Dimension | Hoolachan & Glisson 2010 | 2010 |
| Do not use the intranet for policies regarding the handling of digital evidence | Factor | Hoolachan & Glisson 2010 | 2010 |
| Have a centralized co-ordination point so staff members are clear on who should be contacted | Factor | Hoolachan & Glisson 2010 | 2010 |
| Use an external company to perform forensic analysis but have internal ‘triaging’ capabilities | Factor | Hoolachan & Glisson 2010 | 2010 |
| Business aspects | Dimension | Hoolachan & Glisson 2010 | 2010 |
| Social aspects | Dimension | Hoolachan & Glisson 2010 | 2010 |
| Technical aspects | Dimension | Hoolachan & Glisson 2010 | 2010 |
| Legal apects e.g. admissibility and jurisdiction | Dimension | Hoolachan & Glisson 2010 | 2010 |
| Recognition of the range of personnel within the firm who can be involved in a legal inquiry | Factor | Hoolachan & Glisson 2010 | 2010 |
| Unreasonable expectations of security policy understanding from staff | Factor | Hoolachan & Glisson 2010 | 2010 |
| Automated tools reducing dependence on humans | Factor | Hoolachan & Glisson 2010 | 2010 |
| Too many staff knowing too much detailed security informationFirst responder preparation | Factor | Hoolachan & Glisson 2010 | 2010 |
| Security training | Dimension | Hoolachan & Glisson 2010 | 2010 |
| First response errors | Factor | Hoolachan & Glisson 2010 | 2010 |
| Firm's reputation | Factor | Hoolachan & Glisson 2010 | 2010 |
| Organizational culture | Dimension | Hoolachan & Glisson 2010 | 2010 |
| DF budget | Factor | Hoolachan & Glisson 2010 | 2010 |
| Wireless access | Factor | Ngobeni, Venter & Burke 2010 | 2010 |
| Monitoring | Dimension | Ngobeni, Venter & Burke 2010 | 2010 |
| Logging | Dimension | Ngobeni, Venter & Burke 2010 | 2010 |
| Preservation | Dimension | Ngobeni, Venter & Burke 2010 | 2010 |
| Analysis | Dimension | Ngobeni, Venter & Burke 2010 | 2010 |

| | | | |
|---|---|---|---|
| Report | Dimension | Ngobeni, Venter & Burke 2010 | 2010 |
| Cloud computing | Dimension | Taylor, Haggerty, Gresty & Hegarty 2010 | 2010 |
| Jurisdictional difficulties | Dimension | Taylor, Haggerty, Gresty & Hegarty 2010 | 2010 |
| Encryption | Dimension | Taylor, Haggerty, Gresty & Hegarty 2010 | 2010 |
| Response time | Factor | Taylor, Haggerty, Gresty & Hegarty 2010 | 2010 |
| Availability of an audit trail | Factor | Taylor, Haggerty, Gresty & Hegarty 2010 | 2010 |
| Previous success in recovering from incidents | Factor | Shedden, Ahmad & Ruighaver 2010 | 2010 |
| Resourcing of the incident response capability | Dimension | Shedden, Ahmad & Ruighaver 2010 | 2010 |
| Availability and application of technical expertise | Dimension | Shedden, Ahmad & Ruighaver 2010 | 2010 |
| Support from senior management | Factor | Shedden, Ahmad & Ruighaver 2010 | 2010 |
| Lack of effective learning from incident response | Factor | Shedden, Ahmad & Ruighaver 2010 | 2010 |
| Organizational willingness to update organizational memory | Factor | Shedden, Ahmad & Ruighaver 2010 | 2010 |
| Organizational skill in creating, acquiring and transfering knowledge | Dimension | Shedden, Ahmad & Ruighaver 2010 | 2010 |
| Encouraging both formal, informal and double-loop learning | Factor | Shedden, Ahmad & Ruighaver 2010 | 2010 |
| Enterprise objectives reflected in the security policies | Factor | Pangalos & Ketos 2010 | 2010 |
| Develop and implement a risk-based IS audit strategy | Factor | Pangalos & Ketos 2010 | 2010 |
| Plan audits to ensure that IT and business systems are protected and controlled | Factor | Pangalos & Ketos 2010 | 2010 |
| Conduct audits in accordance with IS audit standards, guidelines and best practices | Factor | Pangalos & Ketos 2010 | 2010 |
| Communicate emerging issues, potential risks and audit results to key stakeholders | Factor | Pangalos & Ketos 2010 | 2010 |
| Advise on the implementation of risk management and control practices | Factor | Pangalos & Ketos 2010 | 2010 |
| Use of cryptographic hashes for dead forensics | Factor | Pangalos & Ketos 2010 | 2010 |
| Ability to distinguish malicious from benign activities | Factor | Pangalos & Ketos 2010 | 2010 |
| Requirement of timeliness of serving electronic documents in court | Factor | Pangalos & Ketos 2010 | 2010 |
| Due diligence and the ability to demonstrate this | Factor | Pangalos & Ketos 2010 | 2010 |
| A dedicated role relating to security and forensics | Factor | Pangalos & Ketos 2010 | 2010 |
| Keeping business continuity (w/o interruption) | Factor | Pangalos, Ilioudis & Pagkalos 2010 | 2010 |
| Benefit/cost proportionality | Factor | Pangalos, Ilioudis & Pagkalos 2010 | 2010 |

| | | | |
|---|---|---|---|
| Corporate security policies | Dimension | Pangalos, Ilioudis & Pagkalos 2010 | 2010 |
| Revisit the risk analysis paradigm | Factor | Pangalos, Ilioudis & Pagkalos 2010 | 2010 |
| Law framework | Dimension | Pangalos, Ilioudis & Pagkalos 2010 | 2010 |
| Security policy | Dimension | Pangalos, Ilioudis & Pagkalos 2010 | 2010 |
| The scene, the requirements, the methodology and tools used, the results and reports | Dimension | Pangalos, Ilioudis & Pagkalos 2010 | 2010 |
| Retained records accessibility | Factor | Pangalos, Ilioudis & Pagkalos 2010 | 2010 |
| Electronic version should accurately represent the original format | Factor | Pangalos, Ilioudis & Pagkalos 2010 | 2010 |
| Meta-data such as author and date should be retained with the record | Factor | Pangalos, Ilioudis & Pagkalos 2010 | 2010 |
| Adapt current Information Security Best Practices to include aspects of Digital Forensic Readiness | Factor | Pangalos, Ilioudis & Pagkalos 2010 | 2010 |
| Support of Good Information Security Governance | Factor | Pangalos, Ilioudis & Pagkalos 2010 | 2010 |
| Integration of Forensics and Audit practice | Factor | Pangalos, Ilioudis & Pagkalos 2010 | 2010 |
| Ability to hold intruders accountable in a court of law and the ability to retaliate | Factor | Pangalos, Ilioudis & Pagkalos 2010 | 2010 |
| Processes related to data backup and recovery | Dimension | Pangalos, Ilioudis & Pagkalos 2010 | 2010 |
| Establish new roles for Forensics | Factor | Pangalos, Ilioudis & Pagkalos 2010 | 2010 |
| Full responsibility and accountability from management | Factor | Pangalos, Ilioudis & Pagkalos 2010 | 2010 |
| Existence of gaps in the SMTP send-receiver pair | Factor | VanStaden & Venter 2010 | 2010 |
| Risk profile of the individual user | Factor | Serra & Venter 2011 | 2011 |
| Adoption of a probe based security monitoring on electronic communications | Factor | VanStaden & Venter 2011 | 2011 |
| Remote web access | Factor | Taylor, Haggerty, Gresty & Lamb 2011 | 2011 |
| Virtualised platform or resource | Factor | Taylor, Haggerty, Gresty & Lamb 2011 | 2011 |
| Independence from hardware and OS profiles | Factor | Taylor, Haggerty, Gresty & Lamb 2011 | 2011 |
| Physical access to the relevant server computer | Factor | Taylor, Haggerty, Gresty & Lamb 2011 | 2011 |
| Encryption | Dimension | Taylor, Haggerty, Gresty & Lamb 2011 | 2011 |
| Lack of standardisation and cross-platform development | Factor | Taylor, Haggerty, Gresty & Lamb 2011 | 2011 |
| To gather admissible evidence legally and without interfering with business processes; | Factor | Valjarevic & Venter 2011 | 2011 |
| To gather evidence targeting the potential crimes and disputes that | Factor | Valjarevic & Venter 2011 | 2011 |

| | | | |
|---|---|---|---|
| may adversely impact an organization; | | | |
| To allow an investigation to proceed at a cost in proportion to the incident; | Factor | Valjarevic & Venter 2011 | 2011 |
| To minimize interruption to the business from any investigation; | Factor | Valjarevic & Venter 2011 | 2011 |
| To ensure that evidence makes a positive impact on the outcome of any legal action. | Factor | Valjarevic & Venter 2011 | 2011 |
| 1. Scenario definition | Factor | Valjarevic & Venter 2011 | 2011 |
| 2. Identification of possible sources of evidence | Factor | Valjarevic & Venter 2011 | 2011 |
| 3. Defining procedures for pre-incident collection, storage and manipulation with data representing possible evidence | Factor | Valjarevic & Venter 2011 | 2011 |
| 4. Defining procedures for pre-incident analyses of data representing possible evidence | Factor | Valjarevic & Venter 2011 | 2011 |
| 5. Defining procedures for incident | Factor | Valjarevic & Venter 2011 | 2011 |
| 6. Defining procedures for post-incident collection, storage and manipulation with data representing possible evidence | Factor | Valjarevic & Venter 2011 | 2011 |
| 7. Defining procedures for post-incident analyses of data representing possible evidence | Factor | Valjarevic & Venter 2011 | 2011 |
| 8. Defining PKI system architecture | Factor | Valjarevic & Venter 2011 | 2011 |
| 9. Implementing defined procedures and PKI system architecture | Dimension | Valjarevic & Venter 2011 | 2011 |
| 10. Assessment of digital forensic readiness implementation | Factor | Valjarevic & Venter 2011 | 2011 |
| There should exist separate log files relating to access (log-in, access to all files) | Factor | Valjarevic & Venter 2011 | 2011 |
| There should exist separate user life-cycle related log | Factor | Valjarevic & Venter 2011 | 2011 |
| There should exist separate PKI services-related logs | Factor | Valjarevic & Venter 2011 | 2011 |
| Lack of technical forensics standardization both in the industry and academia | Factor | Mouhtaropoulos, Grobler & Li 2011 | 2011 |
| Complexity of the information security legal background | Factor | Mouhtaropoulos, Grobler & Li 2011 | 2011 |
| Differences in jurisdictions | Factor | Mouhtaropoulos, Grobler & Li 2011 | 2011 |
| Specifying what needs to be preserved and for which set of events | Factor | Mouhtaropoulos, Grobler & Li 2011 | 2011 |
| Identifying techniques and methodologies | Factor | Mouhtaropoulos, Grobler & Li 2011 | 2011 |
| Organizational policy which will consider the preventative side of security | Dimension | Mouhtaropoulos, Grobler & Li 2011 | 2011 |
| Digital evidence (DE) identification. | Factor | Mouhtaropoulos, Grobler & Li | 2011 |

| | | | |
|---|---|---|---|
| | | 2011 | |
| Risk Assessment by classifying DE exposure and correlating with threats. | Factor | Mouhtaropoulos, Grobler & Li 2011 | 2011 |
| Control to DE access and maintenance of a digital chain of custody (DCOC). | Dimension | Mouhtaropoulos, Grobler & Li 2011 | 2011 |
| Statistical representation of the DE by establishing a Bayesian network; it will calculate the relationship between cost and benefit factors of each measure. | Factor | Mouhtaropoulos, Grobler & Li 2011 | 2011 |
| The events that will escalate an event into a full forensic investigation; the policy should specifically correlate events with the established Bayesian network. | Factor | Mouhtaropoulos, Grobler & Li 2011 | 2011 |
| Evidence Management Plan development | Dimension | Mouhtaropoulos, Grobler & Li 2011 | 2011 |
| Single point of contact (SPOC) establishment with legal authorities. | Factor | Mouhtaropoulos, Grobler & Li 2011 | 2011 |
| Digital forensic investigation (DFI) model choice - the procedure to be followed after an incident occurs. | Factor | Mouhtaropoulos, Grobler & Li 2011 | 2011 |
| Technical infrastructure standards. | Dimension | Mouhtaropoulos, Grobler & Li 2011 | 2011 |
| Staff training procedures on the policy’s contents | Factor | Mouhtaropoulos, Grobler & Li 2011 | 2011 |
| Time period required to perform a digital forensic investigation. | Factor | Mouton & Venter 2011 | 2011 |
| Cost involved in performing a digital forensic investigation. | Factor | Mouton & Venter 2011 | 2011 |
| Ability to collect the evidence without disrupting the environment. | Dimension | Mouton & Venter 2011 | 2011 |
| Acknowledgement packet protocol | Factor | Mouton & Venter 2011 | 2011 |
| Assuring no alteration of intercepted communications | Factor | Mouton & Venter 2011 | 2011 |
| Ability to capture all types of communication | Factor | Mouton & Venter 2011 | 2011 |
| Authenticity and integrity of data packets in capture and store | Factor | Mouton & Venter 2011 | 2011 |
| Verifiability of authenticity and integrity of data packets | Factor | Mouton & Venter 2011 | 2011 |
| Data packets should have a timestamp | Factor | Mouton & Venter 2011 | 2011 |
| Representativity of the sequence of the packets | Factor | Mouton & Venter 2011 | 2011 |
| Implementation of forensic readiness that does not affect current network operation, architecture, transmission frequencies, consumption power, overhead or sensitivity. | Factor | Mouton & Venter 2011 | 2011 |
| Automated live collection of a pre-defined data in the order of volatility and priority, and related to a specific | Factor | Alharbi, Weber-Jahnke & Traore 2011 | 2011 |

| | | | |
|---|---|---|---|
| requirement of an organization | | | |
| Event Triggering Function | Factor | Alharbi, Weber-Jahnke & Traore 2011 | 2011 |
| Automated preservation of the evidence related to the suspicious event, via hashing | Factor | Alharbi, Weber-Jahnke & Traore 2011 | 2011 |
| Automated live analysis of the evidence | Factor | Alharbi, Weber-Jahnke & Traore 2011 | 2011 |
| Use forensics techniques such as data mining to support initial hypothesis of incident | Factor | Alharbi, Weber-Jahnke & Traore 2011 | 2011 |
| Automated report for the proactive component | Factor | Alharbi, Weber-Jahnke & Traore 2011 | 2011 |
| Techniques and automated tools to investigate antiforensics methods | Factor | Alharbi, Weber-Jahnke & Traore 2011 | 2011 |
| Privacy | Dimension | Spyridopoulos & Katos 2011 | 2011 |
| Jurisdiction | Dimension | Spyridopoulos & Katos 2011 | 2011 |
| Cloud storage | Dimension | Spyridopoulos & Katos 2011 | 2011 |
| Legal procedure | Dimension | Spyridopoulos & Katos 2011 | 2011 |
| A block-to-last-chunk name mapping in the cloud | Factor | Spyridopoulos & Katos 2011 | 2011 |
| Persistent storage of chunk location and metadata in a master server | Factor | Spyridopoulos & Katos 2011 | 2011 |
| Weighing costs against risks for implementing DFR | Factor | Reddy, Venter & Olivier 2012 | 2012 |
| Number and amount of activities required for digital forensics | Factor | Reddy, Venter & Olivier 2012 | 2012 |
| Return on security investment (ROSI) | Factor | Reddy, Venter & Olivier 2012 | 2012 |
| Organisational resources coordination | Dimension | Reddy, Venter & Olivier 2012 | 2012 |
| Organization's high level determination | Factor | Reddy, Venter & Olivier 2012 | 2012 |
| Development of IT infrastructure | Dimension | Reddy, Venter & Olivier 2012 | 2012 |
| IT security and DF programmes maturity | Dimension | Reddy, Venter & Olivier 2012 | 2012 |
| Legal requirements | Dimension | Leigh 2012 | 2012 |
| IT systems in use. | Dimension | Leigh 2012 | 2012 |
| Where data is stored. | Factor | Leigh 2012 | 2012 |
| Back-up procedures. | Dimension | Leigh 2012 | 2012 |
| Electronic document retention and archiving policies. | Dimension | Leigh 2012 | 2012 |
| The number of documents likely to be located | Factor | Leigh 2012 | 2012 |
| Tracing custody of individual's devices for upgrades, people's change of office or role. | Factor | Leigh 2012 | 2012 |
| Asset registry for items of electronic equipment that could record information | Factor | Leigh 2012 | 2012 |
| Employment law or privacy issues | Dimension | Leigh 2012 | 2012 |
| Training staff in awareness and incident behavior | Factor | Leigh 2012 | 2012 |

| | | | |
|---|---|---|---|
| Centralization of data | Factor | Leigh 2012 | 2012 |
| Storage in personal devices | Factor | Leigh 2012 | 2012 |
| Determine crimes and disputes the organization is exposed to | Factor | Hamidovic 2012 | 2012 |
| Underestimate the demands that the legal system makes for ensuring admissibility and reliability of digital evidence | Factor | Hamidovic 2012 | 2012 |
| Underestimate how often they may need to produce reliable evidence | Factor | Hamidovic 2012 | 2012 |
| Identify potential evidence based on a risk analysis combined with a cost/benefit approach | Factor | Hamidovic 2012 | 2012 |
| Maturity of information security posture | Factor | Hamidovic 2012 | 2012 |
| Information security auditors' assessment | Factor | Hamidovic 2012 | 2012 |
| Likely threats | Dimension | Hamidovic 2012 | 2012 |
| Sorts of evidence it is likely to need in a civil litigation or criminal proceeding | Factor | Hamidovic 2012 | 2012 |
| How to secure data | Dimension | Hamidovic 2012 | 2012 |
| The amount and quality of evidence already collected | Factor | Hamidovic 2012 | 2012 |
| Legal problems (e.g. admissibility, data protection, human rights, limits to surveillance, obligations to staff members and others, and disclosure in legal proceedings) | Dimension | Hamidovic 2012 | 2012 |
| Management, skill, and resource implications and developed an action plan | Dimension | Hamidovic 2012 | 2012 |
| Information retention | Dimension | Pooe & Labuschagne 2012 | 2012 |
| Response planning | Dimension | Pooe & Labuschagne 2012 | 2012 |
| Training | Dimension | Pooe & Labuschagne 2012 | 2012 |
| Investigation acceleration | Dimension | Pooe & Labuschagne 2012 | 2012 |
| Anonymous activities prevention | Factor | Pooe & Labuschagne 2012 | 2012 |
| Evidence protection | Dimension | Pooe & Labuschagne 2012 | 2012 |
| People | Dimension | Pooe & Labuschagne 2012 | 2012 |
| Process | Dimension | Pooe & Labuschagne 2012 | 2012 |
| Policy | Dimension | Pooe & Labuschagne 2012 | 2012 |
| Technology | Dimension | Pooe & Labuschagne 2012 | 2012 |
| Computer Incident response Team (CIRT) information and skills management | Dimension | Pooe & Labuschagne 2012 | 2012 |
| Security awareness | Dimension | Pooe & Labuschagne 2012 | 2012 |
| Planning of incident response | Dimension | Pooe & Labuschagne 2012 | 2012 |
| Development of investigation methodology | Factor | Pooe & Labuschagne 2012 | 2012 |
| Definition of organizational requirements | Factor | Pooe & Labuschagne 2012 | 2012 |

| | | | |
|---|---|---|---|
| Definition of legal requirements | Factor | Pooe & Labuschagne 2012 | 2012 |
| Existance of reactive and proactive tools | Factor | Pooe & Labuschagne 2012 | 2012 |
| Security/forensic orientation of network design | Factor | Pooe & Labuschagne 2012 | 2012 |
| Modern storage devices own volition in the absence of computer instructions | Factor | Pooe & Labuschagne 2012 | 2012 |
| Hashing tool for authentication of collected data in dead forensics | Factor | Pooe & Labuschagne 2012 | 2012 |
| Tool for authentication of collected data in live forensics | Factor | Pooe & Labuschagne 2012 | 2012 |
| Forensic blurriness affecting fidelity and quantity of evidence acquired in live forensics | Factor | Pooe & Labuschagne 2012 | 2012 |
| Storage technology | Dimension | Pooe & Labuschagne 2012 | 2012 |
| Rising surge of anti-forensic tools | Factor | Pooe & Labuschagne 2012 | 2012 |
| Mature technical environment | Factor | Pooe & Labuschagne 2012 | 2012 |
| Policies & Procedures | Dimension | Pooe & Labuschagne 2012 | 2012 |
| Incident Management | Dimension | Pooe & Labuschagne 2012 | 2012 |
| Response Team | Factor | Pooe & Labuschagne 2012 | 2012 |
| Securing the evidence without contaminating it | Factor | Pooe & Labuschagne 2012 | 2012 |
| Acquiring the evidence without altering or damaging the original | Factor | Pooe & Labuschagne 2012 | 2012 |
| Authenticating that the recovered evidence is the same as the original seized data | Factor | Pooe & Labuschagne 2012 | 2012 |
| Analysing the data without modifying it | Factor | Pooe & Labuschagne 2012 | 2012 |
| Management commitment and leadership to secure information systems | Dimension | Elachgar, Boulafdour, Makoudi & Regragui 2012 | 2012 |
| The adoption of standards for information security | Factor | Elachgar, Boulafdour, Makoudi & Regragui 2012 | 2012 |
| User awareness of the issues, threats and best practices in information security | Dimension | Elachgar, Boulafdour, Makoudi & Regragui 2012 | 2012 |
| The implementation of policies, processes and procedures to secure the information system | Dimension | Elachgar, Boulafdour, Makoudi & Regragui 2012 | 2012 |
| Adequate technology to secure the information system | Dimension | Elachgar, Boulafdour, Makoudi & Regragui 2012 | 2012 |
| Compliance with regulatory requirements according to information security information | Dimension | Elachgar, Boulafdour, Makoudi & Regragui 2012 | 2012 |
| Establishment of a dashboard of measurement and control of the security information | Factor | Elachgar, Boulafdour, Makoudi & Regragui 2012 | 2012 |
| Risk analysis | Dimension | Elachgar, Boulafdour, Makoudi & Regragui 2012 | 2012 |
| Measure maturity of repositories of information | Factor | Elachgar, Boulafdour, Makoudi & Regragui 2012 | 2012 |

| | | | |
|---|---|---|---|
| Security indicators | Dimension | Elachgar, Boulafdour, Makoudi & Regragui 2012 | 2012 |
| Check security through audits | Factor | Elachgar, Boulafdour, Makoudi & Regragui 2012 | 2012 |
| Penetration tests | Factor | Elachgar, Boulafdour, Makoudi & Regragui 2012 | 2012 |
| Security benchmark | Factor | Elachgar, Boulafdour, Makoudi & Regragui 2012 | 2012 |
| Security of premises | Dimension | Elachgar, Boulafdour, Makoudi & Regragui 2012 | 2012 |
| Architecture and Systems Security | Dimension | Elachgar, Boulafdour, Makoudi & Regragui 2012 | 2012 |
| Application security | Factor | Elachgar, Boulafdour, Makoudi & Regragui 2012 | 2012 |
| Development of action plans | Dimension | Elachgar, Boulafdour, Makoudi & Regragui 2012 | 2012 |
| Cloud service's systems functionality | Factor | Ferguson-Boucher & Endicott-Popovsky 2012 | 2012 |
| Records management including the cloud | Dimension | Ferguson-Boucher & Endicott-Popovsky 2012 | 2012 |
| Information governance and assurance (confidentiality, integrity, availability, authentication and non-repudiation) | Dimension | Ferguson-Boucher & Endicott-Popovsky 2012 | 2012 |
| Appraisal strategies | Factor | Ferguson-Boucher & Endicott-Popovsky 2012 | 2012 |
| Retention schedules | Factor | Ferguson-Boucher & Endicott-Popovsky 2012 | 2012 |
| Disposition plans | Factor | Ferguson-Boucher & Endicott-Popovsky 2012 | 2012 |
| Assuring the records posses content, context and structure | Factor | Ferguson-Boucher & Endicott-Popovsky 2012 | 2012 |
| Assuring records authenticity, reliability, integrity and usability | Factor | Ferguson-Boucher & Endicott-Popovsky 2012 | 2012 |
| Identify where to look in the system | Factor | Ferguson-Boucher & Endicott-Popovsky 2012 | 2012 |
| Identify how to store and for how long | Factor | Ferguson-Boucher & Endicott-Popovsky 2012 | 2012 |
| Data retrieval mechanism | Factor | Ferguson-Boucher & Endicott-Popovsky 2012 | 2012 |
| Tamper-proof mechanism | Factor | Ferguson-Boucher & Endicott-Popovsky 2012 | 2012 |
| Create evidence | Factor | Ferguson-Boucher & Endicott-Popovsky 2012 | 2012 |
| Capture evidence | Factor | Ferguson-Boucher & Endicott-Popovsky 2012 | 2012 |
| Organize evidence | Factor | Ferguson-Boucher & Endicott-Popovsky 2012 | 2012 |
| Pluralize evidence | Factor | Ferguson-Boucher & Endicott-Popovsky 2012 | 2012 |
| Assessing evidence for evidential weight | Factor | Ferguson-Boucher & Endicott-Popovsky 2012 | 2012 |
| Curation of evidence movement through time | Factor | Ferguson-Boucher & Endicott-Popovsky 2012 | 2012 |
| Patterns of physical traces and imprints (logs, audits) | Factor | Ferguson-Boucher & Endicott-Popovsky 2012 | 2012 |

|  |  |  |  |
|---|---|---|---|
| Manifestation of evidence | Factor | Ferguson-Boucher & Endicott-Popovsky 2012 | 2012 |
| Calibration audits | Factor | Ferguson-Boucher & Endicott-Popovsky 2012 | 2012 |
| Chain of custody is kept for the evidence | Dimension | Ferguson-Boucher & Endicott-Popovsky 2012 | 2012 |
| Cross-disciplinary teams | Dimension | Ferguson-Boucher & Endicott-Popovsky 2012 | 2012 |
| Senser location near key assets | Factor | Ferguson-Boucher & Endicott-Popovsky 2012 | 2012 |
| IDS | Factor | Ferguson-Boucher & Endicott-Popovsky 2012 | 2012 |
| Monitoring of regulation and legislation | Factor | Ferguson-Boucher & Endicott-Popovsky 2012 | 2012 |
| The preservation, continuity, mainainability and resilience of cloud information | Dimension | Ferguson-Boucher & Endicott-Popovsky 2012 | 2012 |
| Relocate critical assets for better management | Factor | Ferguson-Boucher & Endicott-Popovsky 2012 | 2012 |
| Keeping association of data to metadata when moving to the cloud | Factor | Ferguson-Boucher & Endicott-Popovsky 2012 | 2012 |
| Monitoring organizational regulations compliance when moving to the cloud | Factor | Ferguson-Boucher & Endicott-Popovsky 2012 | 2012 |
| Cloud warehousing | Dimension | Ferguson-Boucher & Endicott-Popovsky 2012 | 2012 |
| Legal framework and jurisdictions | Dimension | Ferguson-Boucher & Endicott-Popovsky 2012 | 2012 |
| Generally accepted standardized training and certification programs | Dimension | Mouhtaropoulos & Li 2012 | 2012 |
| Daubert test of technique (tested, peer reviewed, error rate and accepted) | Factor | Mouhtaropoulos & Li 2012 | 2012 |
| Policies from yasinsac & Manzano | Dimension | Mouhtaropoulos & Li 2012 | 2012 |
| Digital assets value assessment | Factor | Mouhtaropoulos & Li 2012 | 2012 |
| Risk assessment | Dimension | Mouhtaropoulos & Li 2012 | 2012 |
| Digital assets filtering | Factor | Mouhtaropoulos & Li 2012 | 2012 |
| Data identification | Dimension | Mouhtaropoulos & Li 2012 | 2012 |
| Forensic policy writing and Legal review | Dimension | Mouhtaropoulos & Li 2012 | 2012 |
| Forensic policy ensurance | Factor | Mouhtaropoulos & Li 2012 | 2012 |
| Digital evidence management | Dimension | Mouhtaropoulos & Li 2012 | 2012 |
| Incident response process | Dimension | Mouhtaropoulos & Li 2012 | 2012 |
| Staff training | Dimension | Mouhtaropoulos & Li 2012 | 2012 |
| Identify sources of potential evidence | Factor | Mouhtaropoulos & Li 2012 | 2012 |
| Calculate value of digital evidence | Factor | Mouhtaropoulos & Li 2012 | 2012 |
| Correlate potential sources with threats | Factor | Mouhtaropoulos & Li 2012 | 2012 |
| Calculate level of digital evidence exposure to threats | Factor | Mouhtaropoulos & Li 2012 | 2012 |
| Conduct assessment of digital evidence from its value and exposure | Factor | Mouhtaropoulos & Li 2012 | 2012 |

|  |  |  |  |
|---|---|---|---|
| Identify potential cost of measures and threats | Factor | Mouhtaropoulos & Li 2012 | 2012 |
| Identify potential benefit of measures | Factor | Mouhtaropoulos & Li 2012 | 2012 |
| Relate cost and benefits trhough a Bayesian Network | Factor | Mouhtaropoulos & Li 2012 | 2012 |
| Conduct Cost-Benefit Analysis of measures and threats | Factor | Mouhtaropoulos & Li 2012 | 2012 |
| Depict results on a Cost-Benefit factor relation model | Dimension | Mouhtaropoulos & Li 2012 | 2012 |
| Choose a forensic investigation model to perform after incident | Factor | Mouhtaropoulos & Li 2012 | 2012 |
| Develop chain of custody | Factor | Mouhtaropoulos & Li 2012 | 2012 |
| Decide on trigger event of full DF investigation | Factor | Mouhtaropoulos & Li 2012 | 2012 |
| Decide on single point of contact with authorities | Factor | Mouhtaropoulos & Li 2012 | 2012 |
| Prioritization model | Factor | Mouhtaropoulos & Li 2012 | 2012 |
| Business continuity plan | Factor | Mouhtaropoulos & Li 2012 | 2012 |
| System monitoring | Factor | VanStaden & Venter 2012 | 2012 |
| Risk Assessment | Dimension | Mouhtaropoulos, Dimotikalis & Li 2013 | 2013 |
| Digital Evidence Management | Dimension | Mouhtaropoulos, Dimotikalis & Li 2013 | 2013 |
| Staff Training | Dimension | Mouhtaropoulos, Dimotikalis & Li 2013 | 2013 |
| Incident Response Process | Dimension | Mouhtaropoulos, Dimotikalis & Li 2013 | 2013 |
| Policies & Procedures | Dimension | Mouhtaropoulos, Dimotikalis & Li 2013 | 2013 |
| Business Scenarios | Dimension | Mouhtaropoulos, Dimotikalis & Li 2013 | 2013 |
| Digital Evidence Preparation | Dimension | Mouhtaropoulos, Dimotikalis & Li 2013 | 2013 |
| IR Team Preparation | Factor | Mouhtaropoulos, Dimotikalis & Li 2013 | 2013 |
| Response Toolkit Preparation | Factor | Mouhtaropoulos, Dimotikalis & Li 2013 | 2013 |
| Legal review | Factor | Mouhtaropoulos, Dimotikalis & Li 2013 | 2013 |
| Tracing back the actions of each employee | Factor | Mouhtaropoulos, Dimotikalis & Li 2013 | 2013 |
| Human factor | Dimension | Mouhtaropoulos, Dimotikalis & Li 2013 | 2013 |
| Specific methodology to capture, stored, analyze, preserve, integrate, present evidence | Dimension | Mouhtaropoulos, Li & Grobler 2012 | 2012 |
| Relevant software tools to capture, stored, analyze, preserve, integrate, present evidence | Dimension | Mouhtaropoulos, Li & Grobler 2012 | 2012 |
| Outsourcing costs | Factor | Mouhtaropoulos, Li & Grobler 2012 | 2012 |
| Risk assessment analysis | Dimension | Mouhtaropoulos, Li & Grobler 2012 | 2012 |
| Regulatory framework meeting | Factor | Mouhtaropoulos, Li & Grobler | 2012 |

|  |  |  |  |
|---|---|---|---|
| organizational needs |  | 2012 |  |
| Cost-benefit analysis of compliance costs vs. value-added proactive security benefits | Factor | Mouhtaropoulos, Li & Grobler 2012 | 2012 |
| Event analysis | Dimension | Reddy & Venter 2013 | 2013 |
| DFR information | Dimension | Reddy & Venter 2013 | 2013 |
| Costing | Dimension | Reddy & Venter 2013 | 2013 |
| Access control | Factor | Reddy & Venter 2013 | 2013 |
| User interface | Factor | Reddy & Venter 2013 | 2013 |
| Staff from multiple departments and business units | Dimension | Reddy & Venter 2013 | 2013 |
| Network infrastructure and computing platforms | Dimension | Reddy & Venter 2013 | 2013 |
| Monitor or log network and host activity | Factor | Reddy & Venter 2013 | 2013 |
| Secure storage of logs | Factor | Reddy & Venter 2013 | 2013 |
| Distinguish whether hardware or software elements are being monitored | Factor | Reddy & Venter 2013 | 2013 |
| Automated alarm upon detection of potential or actual incident | Factor | Reddy & Venter 2013 | 2013 |
| Configuration procedures for monitoring and logging | Factor | Reddy & Venter 2013 | 2013 |
| Investigative teams (DF teams) and incident response teams descriptions | Dimension | Reddy & Venter 2013 | 2013 |
| Training requirements and training | Dimension | Reddy & Venter 2013 | 2013 |
| Business process descriptions | Dimension | Reddy & Venter 2013 | 2013 |
| Organisational DF policies and policies related to DFR | Dimension | Reddy & Venter 2013 | 2013 |
| Existence of a suspicion policy | Factor | Reddy & Venter 2013 | 2013 |
| Law enforcement contact policy | Factor | Reddy & Venter 2013 | 2013 |
| Escalation procedures | Factor | Reddy & Venter 2013 | 2013 |
| Incident response procedure | Dimension | Reddy & Venter 2013 | 2013 |
| Law enforcement contact procedure | Factor | Reddy & Venter 2013 | 2013 |
| Defined organisational structure, privileges and rank hierarchy | Dimension | Reddy & Venter 2013 | 2013 |
| Staff involved in DFR and incident response | Dimension | Reddy & Venter 2013 | 2013 |
| Intrusion detection systems (IDS) | Factor | Reddy & Venter 2013 | 2013 |
| Security event management software (SEM) | Factor | Reddy & Venter 2013 | 2013 |
| Incident management software | Factor | Reddy & Venter 2013 | 2013 |
| Storage of information about training, procedures, people, roles, policies, etc. | Dimension | Reddy & Venter 2013 | 2013 |
| Documentation of incidents and investigation archive | Dimension | Reddy & Venter 2013 | 2013 |
| Leave management | Factor | Reddy & Venter 2013 | 2013 |
| Organization size | Factor | Reddy & Venter 2013 | 2013 |
| Organization industry | Factor | Reddy & Venter 2013 | 2013 |

| | | | |
|---|---|---|---|
| Multi-jurisdictions | Factor | Sibiya, Venter & Ngobeni 2013 | 2013 |
| Multi-tenants of data | Factor | Sibiya, Venter & Ngobeni 2013 | 2013 |
| A lack of forensic readiness mechanisms in cloud infrastructures | Factor | Sibiya, Venter & Ngobeni 2013 | 2013 |
| Escalation of costs | Factor | Sibiya, Venter & Ngobeni 2013 | 2013 |
| Applications layer that interact with layer 7 of the ISO/OSI model (e.g. static and dynamic web applications, web clients, web servers, application servers and web services | Factor | Sibiya, Venter & Ngobeni 2013 | 2013 |
| Ram forensics | Factor | Sibiya, Venter & Ngobeni 2013 | 2013 |
| Network forensics | Dimension | Sibiya, Venter & Ngobeni 2013 | 2013 |
| Computer forensics | Dimension | Sibiya, Venter & Ngobeni 2013 | 2013 |
| Centralized logging | Factor | Trenwith & Venter 2013 | 2013 |
| Data and Process provenance | Dimension | Trenwith & Venter 2013 | 2013 |
| The proportionality rule to collect only useful evidence upon good cause | Factor | Trenwith & Venter 2013 | 2013 |
| Integrity of the evidence and chain of custody | Dimension | Trenwith & Venter 2013 | 2013 |
| Difficulty of device isolation in the cloud | Factor | Trenwith & Venter 2013 | 2013 |
| Jurisdictional issues | Dimension | Trenwith & Venter 2013 | 2013 |
| Decreased control over data and decreased access to forensic data from a client side | Factor | Trenwith & Venter 2013 | 2013 |
| Access control on the central server | Factor | Trenwith & Venter 2013 | 2013 |
| Cloudification | Dimension | Trenwith & Venter 2013 | 2013 |
| Communication Channel | Factor | Trenwith & Venter 2013 | 2013 |
| Encryption | Dimension | Trenwith & Venter 2013 | 2013 |
| Compression | Factor | Trenwith & Venter 2013 | 2013 |
| Authentication of log data and proof of integrity | Factor | Trenwith & Venter 2013 | 2013 |
| Authenticating the client and server | Factor | Trenwith & Venter 2013 | 2013 |
| Timestamping | Factor | Trenwith & Venter 2013 | 2013 |
| Qualified individuals | Dimension | Elyas, Maynard, Ahmad & Lonie 2014 | 2014 |
| Forensic strategy | Dimension | Elyas, Maynard, Ahmad & Lonie 2014 | 2014 |
| Non-technical stakeholders | Dimension | Elyas, Maynard, Ahmad & Lonie 2014 | 2014 |
| Technical stakeholders | Dimension | Elyas, Maynard, Ahmad & Lonie 2014 | 2014 |
| Technology | Dimension | Elyas, Maynard, Ahmad & Lonie 2014 | 2014 |
| Monitoring | Dimension | Elyas, Maynard, Ahmad & Lonie 2014 | 2014 |
| Architecture | Dimension | Elyas, Maynard, Ahmad & Lonie 2014 | 2014 |
| Policies | Dimension | Elyas, Maynard, Ahmad & Lonie 2014 | 2014 |

| | | | |
|---|---|---|---|
| Training | Dimension | Elyas, Maynard, Ahmad & Lonie 2014 | 2014 |
| Forensic culture | Dimension | Elyas, Maynard, Ahmad & Lonie 2014 | 2014 |
| Top management support | Factor | Elyas, Maynard, Ahmad & Lonie 2014 | 2014 |
| Governance | Dimension | Elyas, Maynard, Ahmad & Lonie 2014 | 2014 |
| Need of regulatory compliance | Factor | Elyas, Maynard, Ahmad & Lonie 2014 | 2014 |
| Need of internal investigations | Factor | Elyas, Maynard, Ahmad & Lonie 2014 | 2014 |
| Involvement in legal proceedings | Factor | Elyas, Maynard, Ahmad & Lonie 2014 | 2014 |
| Data indexing | Factor | Elyas, Maynard, Ahmad & Lonie 2014 | 2014 |
| Information fusion | Factor | Elyas, Maynard, Ahmad & Lonie 2014 | 2014 |
| Cryptographic Time-stamps | Factor | Elyas, Maynard, Ahmad & Lonie 2014 | 2014 |
| System synchronization | Factor | Elyas, Maynard, Ahmad & Lonie 2014 | 2014 |
| Digital signatures | Factor | Elyas, Maynard, Ahmad & Lonie 2014 | 2014 |
| File hashing | Factor | Elyas, Maynard, Ahmad & Lonie 2014 | 2014 |
| Maintaining change management database | Factor | Elyas, Maynard, Ahmad & Lonie 2014 | 2014 |
| CCTVs | Factor | Elyas, Maynard, Ahmad & Lonie 2014 | 2014 |
| Encryption | Dimension | Elyas, Maynard, Ahmad & Lonie 2014 | 2014 |
| Hashing | Factor | Elyas, Maynard, Ahmad & Lonie 2014 | 2014 |
| Remote secure central servers for logs | Factor | Elyas, Maynard, Ahmad & Lonie 2014 | 2014 |
| IDS | Factor | Elyas, Maynard, Ahmad & Lonie 2014 | 2014 |
| Anti-virus and Anti-Spyware | Factor | Elyas, Maynard, Ahmad & Lonie 2014 | 2014 |
| Communications with external stakeholders | Dimension | Elyas, Maynard, Ahmad & Lonie 2014 | 2014 |
| Leadership commitment towards the forensic program | Factor | Elyas, Maynard, Ahmad & Lonie 2014 | 2014 |
| Appropriate organizational structure that takes forensics into account | Dimension | Elyas, Maynard, Ahmad & Lonie 2014 | 2014 |
| Staff awareness | Dimension | Elyas, Maynard, Ahmad & Lonie 2014 | 2014 |
| Enforcement of policies | Factor | Elyas, Maynard, Ahmad & Lonie 2014 | 2014 |
| Identify the objectives of forensic program | Factor | Elyas, Maynard, Ahmad & Lonie 2014 | 2014 |
| Identify potential scenarios that will require digital evidence | Factor | Elyas, Maynard, Ahmad & Lonie 2014 | 2014 |
| Identify and prioritize evidence sources | Factor | Elyas, Maynard, Ahmad & Lonie 2014 | 2014 |

| | | | |
|---|---|---|---|
| Identify forensic roles | Factor | Elyas, Maynard, Ahmad & Lonie 2014 | 2014 |
| Plan for budget | Factor | Elyas, Maynard, Ahmad & Lonie 2014 | 2014 |
| Capabilities of legal evidence management | Dimension | Elyas, Maynard, Ahmad & Lonie 2014 | 2014 |
| Capabilities of internal investigations | Dimension | Elyas, Maynard, Ahmad & Lonie 2014 | 2014 |
| Capabilities of regulatory compliance | Dimension | Elyas, Maynard, Ahmad & Lonie 2014 | 2014 |
| Is there intelligence in place? | Factor | Web, Ahmad, Maynard / Shanks 2014 | 2014 |
| Security awareness | Dimension | Web, Ahmad, Maynard / Shanks 2014 | 2014 |
| Personnel believe in the necessity of technology such as anti-spyware | Factor | Web, Ahmad, Maynard / Shanks 2014 | 2014 |
| Personnel understand the technology | Dimension | Web, Ahmad, Maynard / Shanks 2014 | 2014 |
| Impact on stakeholders (e.g. customers and employees) | Factor | Starkman 2014 | 2014 |
| Provide data that is triangulated with other data, and to be able to prove timeline | Factor | Elyas, Ahmad, Maynard & Lonie 2015 | 2015 |
| Knowing what information you have | Factor | Elyas, Ahmad, Maynard & Lonie 2015 | 2015 |
| Knowing where information is stored | Factor | Elyas, Ahmad, Maynard & Lonie 2015 | 2015 |
| Knowing who is in charge of the information | Factor | Elyas, Ahmad, Maynard & Lonie 2015 | 2015 |
| Objective of DFR program e.g. business objectives, compliance, internal investigation, forensic response, and legal evidence management | Dimension | Elyas, Ahmad, Maynard & Lonie 2015 | 2015 |
| Business objectives e.g. Satisfaying de directors and Corporate reputation | Factor | Elyas, Ahmad, Maynard & Lonie 2015 | 2015 |
| Organizational Factors (Top Management Support, Governance, Culture) Elyas 2014 | Dimension | Elyas, Ahmad, Maynard & Lonie 2015 | 2015 |
| Roles instead of positions (Forensic stakeholder instead of Technical stakeholder) | Factor | Elyas, Ahmad, Maynard & Lonie 2015 | 2015 |
| Extent to which design & configuration of IT architecture complements forensic process | Factor | Elyas, Ahmad, Maynard & Lonie 2015 | 2015 |
| Having logging features architected for digital forensics | Factor | Elyas, Ahmad, Maynard & Lonie 2015 | 2015 |
| Validated forensic tools | Dimension | Elyas, Ahmad, Maynard & Lonie 2015 | 2015 |
| Transparency | Factor | Elyas, Ahmad, Maynard & Lonie 2015 | 2015 |
| Maintenance and testing of systems | Dimension | Elyas, Ahmad, Maynard & Lonie 2015 | 2015 |
| Need for adequate resources to sustain the forensic readiness | Factor | Elyas, Ahmad, Maynard & Lonie 2015 | 2015 |

|  |  |  |  |
|---|---|---|---|
| program |  |  |  |
| Senior management buy-in | Factor | Elyas, Ahmad, Maynard & Lonie 2015 | 2015 |
| Ability to recover assets, or avoiding financial loss | Factor | Elyas, Ahmad, Maynard & Lonie 2015 | 2015 |
| Certified or validated technology | Factor | Elyas, Ahmad, Maynard & Lonie 2015 | 2015 |
| Practice and experience with technology | Factor | Elyas, Ahmad, Maynard & Lonie 2015 | 2015 |
| Updated technology | Factor | Elyas, Ahmad, Maynard & Lonie 2015 | 2015 |
| Cost of technology | Factor | Elyas, Ahmad, Maynard & Lonie 2015 | 2015 |
| Resourcing | Dimension | Elyas, Ahmad, Maynard & Lonie 2015 | 2015 |
| Technology use and selection | Dimension | Elyas, Ahmad, Maynard & Lonie 2015 | 2015 |
| Forensic Training | Dimension | Elyas, Ahmad, Maynard & Lonie 2015 | 2015 |
| Legal investigations | Factor | Elyas, Ahmad, Maynard & Lonie 2015 | 2015 |
| Incident response | Factor | Elyas, Ahmad, Maynard & Lonie 2015 | 2015 |
| Policy | Dimension | Elyas, Ahmad, Maynard & Lonie 2015 | 2015 |
| Training in the of use forensic tools | Factor | Elyas, Ahmad, Maynard & Lonie 2015 | 2015 |
| Training about the Forensic Policy and how to recognise and respond to an incident | Factor | Elyas, Ahmad, Maynard & Lonie 2015 | 2015 |
| Leadership commitment towards forensics | Factor | Elyas, Ahmad, Maynard & Lonie 2015 | 2015 |
| Staff awareness and commitment towards forensics | Factor | Elyas, Ahmad, Maynard & Lonie 2015 | 2015 |
| Organisational structure that takes forensics into consideration | Dimension | Elyas, Ahmad, Maynard & Lonie 2015 | 2015 |
| Enforcement of forensic policy and training | Factor | Elyas, Ahmad, Maynard & Lonie 2015 | 2015 |
| Accountability of staff towards their forensic responsibilities | Factor | Elyas, Ahmad, Maynard & Lonie 2015 | 2015 |
| Active monitoring and continuous assessment of system activities | Factor | Elyas, Ahmad, Maynard & Lonie 2015 | 2015 |
| Type of data | Factor | Diaz Lopez | 2014 |
| Potential sources of attacks or failure | Factor | Diaz Lopez | 2014 |
| Number of customers | Factor | Diaz Lopez | 2014 |
| Sales | Factor | Diaz Lopez | 2014 |
| Location | Factor | Diaz Lopez | 2014 |
| Preparedness of competitors and enemies | Factor | Diaz Lopez | 2014 |
| BYOD policies | Factor | Diaz Lopez | 2014 |
| Is it data or metadata? | Factor | Diaz Lopez | 2014 |
| Is it part of the content? | Factor | Diaz Lopez | 2014 |
| Is it a dimension or a measure? | Factor | Diaz Lopez | 2014 |

| | | | |
|---|---|---|---|
| Can it be derived? | Factor | Diaz Lopez | 2014 |
| What other data are related to it? | Factor | Diaz Lopez | 2014 |
| Is it legal to store or view? | Factor | Diaz Lopez | 2014 |
| Where else the data are? | Factor | Diaz Lopez | 2014 |
| Concern about corporate image | Factor | Diaz Lopez | 2014 |
| Perceptions of security risk | Factor | Diaz Lopez | 2014 |
| Culture or requirements of corporate secrecy | Factor | Diaz Lopez | 2014 |
| Past successes in dealing with digital forensics incidents | Factor | Diaz Lopez | 2014 |
| Business continuity is critical | Factor | Diaz Lopez | 2014 |
| Completeness of the DFR framework itself | Factor | Diaz Lopez | 2014 |
| Timing of events | Factor | Diaz Lopez | 2014 |

# APPENDIX B - ITEMS CLASSIFIED AS DIMENSIONS

| Item | Re-Classification | Paper |
|---|---|---|
| Security policy | Dimension | VonSolms 2000 / DIS ISO/IEC 17799 - 1 (BS 7799) |
| Security organization | Dimension | VonSolms 2000 / DIS ISO/IEC 17799 - 1 (BS 7799) |
| Personnel security | Dimension | VonSolms 2000 / DIS ISO/IEC 17799 - 1 (BS 7799) |
| Physical and environmental security | Dimension | VonSolms 2000 / DIS ISO/IEC 17799 - 1 (BS 7799) |
| Communications and operations | Dimension | VonSolms 2000 / DIS ISO/IEC 17799 - 1 (BS 7799) |
| Management | Dimension | VonSolms 2000 / DIS ISO/IEC 17799 - 1 (BS 7799) |
| Systems development and maintenance | Dimension | VonSolms 2000 / DIS ISO/IEC 17799 - 1 (BS 7799) |
| Business Continuity management | Dimension | VonSolms 2000 / DIS ISO/IEC 17799 - 1 (BS 7799) |
| Compliance | Dimension | VonSolms 2000 / DIS ISO/IEC 17799 - 1 (BS 7799) |
| Cultivating an Information Security Culture Right | Dimension | VonSolms 2000 |
| Tools & Equipment | Dimension | US DoS/NIJ 2001 |
| Evidence Collection | Dimension | US DoS/NIJ 2001 |
| Packaging, Transportation, and Storage | Dimension | US DoS/NIJ 2001 |
| Forensic Acquisition | Dimension | Tan 2001 |
| Evidence Handling | Dimension | Tan 2001 |
| Chain of custody | Dimension | Tan 2001 |
| Transport and encryption | Dimension | Tan 2001 |
| Physical storage & transport of evidence | Dimension | Tan 2001 |
| Planning the response. | Dimension | Yasinsac & Manzano 2001 |
| Training. | Dimension | Yasinsac & Manzano 2001 |
| Accelerating the investigation. | Dimension | Yasinsac & Manzano 2001 |
| Protect the evidence. | Dimension | Yasinsac & Manzano 2001 |
| Information States | Dimension | Maconachy, Schou, Ragsdale & Welch 2001 |
| Security Services | Dimension | Maconachy, Schou, Ragsdale & Welch 2001 |
| Security Countermeasures | Dimension | Maconachy, Schou, Ragsdale & Welch 2001 |
| Time | Dimension | Maconachy, Schou, Ragsdale & Welch 2001 |
| Education | Dimension | Maconachy, Schou, Ragsdale & Welch 2001 |
| Training. | Dimension | Maconachy, Schou, Ragsdale & Welch 2001 |
| Literacy | Dimension | Maconachy, Schou, Ragsdale & Welch 2001 |

|  |  |  |
|---|---|---|
| Awareness | Dimension | Maconachy, Schou, Ragsdale & Welch 2001 |
| Reliable unbiased methods to extract and analyze evidence | Dimension | Reith, Carr & Gunch 2002 |
| Storage technology | Dimension | Reith, Carr & Gunch 2002 |
| Chain of custody | Dimension | Reith, Carr & Gunch 2002 |
| Infrastructure digital and physical | Dimension | Carrier & Spafford 2003 |
| Operations | Dimension | Carrier & Spafford 2003 |
| Training | Dimension | Carrier & Spafford 2003 |
| Equipment | Dimension | Carrier & Spafford 2003 |
| Maintenance of the target environment | Dimension | Carrier & Spafford 2003 |
| How can we be sure that there even was an incident? | Dimension | Stephenson 2003 |
| What legal issues need to be addressed (policies, privacy, subpoenas, warrants, etc.)? | Dimension | Stephenson 2003 |
| What non-technical (business) issues impacted the success or failure of the attack? | Dimension | Stephenson 2003 |
| Logs from involved computers, detection systems, firewalls, etc. | Dimension | Stephenson 2003 / Daubert test |
| A. Identification | Dimension | DFRWS cited by Stephenson 2003 |
| A6. System | Dimension | DFRWS cited by Stephenson 2003 |
| A7. Monitoring Audit Analysis | Dimension | DFRWS cited by Stephenson 2003 |
| B. Preservation | Dimension | DFRWS cited by Stephenson 2003 |
| B1. Case Management | Dimension | DFRWS cited by Stephenson 2003 |
| B3. Chain of Custody | Dimension | DFRWS cited by Stephenson 2003 |
| C. Collection | Dimension | DFRWS cited by Stephenson 2003 |
| C1. Preservation | Dimension | DFRWS cited by Stephenson 2003 |
| C2. Approved Methods | Dimension | DFRWS cited by Stephenson 2003 |
| C3. Approved Software | Dimension | DFRWS cited by Stephenson 2003 |
| C4.Approved Hardware | Dimension | DFRWS cited by Stephenson 2003 |
| C5. Legal Authority | Dimension | DFRWS cited by Stephenson 2003 |
| D. Examination | Dimension | DFRWS cited by Stephenson 2003 |
| D1. Preservation | Dimension | DFRWS cited by Stephenson 2003 |
| E. Analysis | Dimension | DFRWS cited by Stephenson 2003 |
| E1. Preservation | Dimension | DFRWS cited by Stephenson 2003 |
| E2. Traceability | Dimension | DFRWS cited by Stephenson 2003 |
| E6. Timeline | Dimension | DFRWS cited by Stephenson 2003 |
| E8. Spatial | Dimension | DFRWS cited by Stephenson 2003 |
| F. Presentation | Dimension | DFRWS cited by Stephenson 2003 |
| F1. Documentation | Dimension | DFRWS cited by Stephenson 2003 |
| Codes of conduct and security policies | Dimension | Wolfe-Wilson & Wolfe 2003 |
| Chain of evidence | Dimension | Wolfe-Wilson & Wolfe 2003 |
| Laboratory and specialized hardware and software | Dimension | Wolfe-Wilson & Wolfe 2003 |

| | | |
|---|---|---|
| Chain of custody | Dimension | Bradford, Brown, Perdue & Self 2004 |
| Infrastructure | Dimension | Carrier & Spafford 2004 |
| Preservation of physical and digital evidence | Dimension | Carrier & Spafford 2004 |
| 3. Planning | Dimension | Ciardhuáin 2004 |
| 4. Notification | Dimension | Ciardhuáin 2004 |
| 5. Search for and identify evidence | Dimension | Ciardhuáin 2004 |
| 6. Collection of evidence | Dimension | Ciardhuáin 2004 |
| 7. Transport of evidence | Dimension | Ciardhuáin 2004 |
| 8. Storage of evidence | Dimension | Ciardhuáin 2004 |
| 9. Examination of evidence | Dimension | Ciardhuáin 2004 |
| 10. Hypothesis | Dimension | Ciardhuáin 2004 |
| 11. Presentation of hypothesis | Dimension | Ciardhuáin 2004 |
| 12. Proof/Defense of hypothesis | Dimension | Ciardhuáin 2004 |
| 13. Dissemination of information | Dimension | Ciardhuáin 2004 |
| Information flow and controls | Dimension | Ciardhuáin 2004 |
| Cost | Dimension | Rowlingson 2004 |
| 4. How is data currently controlled, secured and managed? | Dimension | Rowlingson 2004 |
| 12. How could data be made available to an investigation? | Dimension | Rowlingson 2004 |
| Capability for securely gathering legally admissible evidence | Dimension | Rowlingson 2004 |
| Establishment of policies for secure storage and handling of potential evidence | Dimension | Rowlingson 2004 |
| Monitoring of incidents detection and deterrence systems | Dimension | Rowlingson 2004 |
| Train personnel in incident awareness, roles and legal aspects of digital evidence process | Dimension | Rowlingson 2004 |
| Benefit/cost proportionality | Dimension | Rowlingson 2004 |
| Evidence collection requirements | Dimension | Rowlingson 2004 |
| Retention of information | Dimension | Rowlingson 2004 |
| Planning of the response | Dimension | Rowlingson 2004 |
| Training | Dimension | Rowlingson 2004 |
| Acceleration of the investigation | Dimension | Rowlingson 2004 |
| Legal | Dimension | Rowlingson 2004 |
| Technical | Dimension | Rowlingson 2004 |
| Non-technical | Dimension | Rowlingson 2004 |
| Personnel and external organizations | Dimension | Rowlingson 2004 |
| Understanding possible evidence sources, how to gather evidence legally and cost-effectively, when to escalate into a formal investigation, and how to put together a case involving law enforcement agencies. | Dimension | Rowlingson 2004 |
| Legal requirements and constraints on collection and preservation of potential digital evidence | Dimension | Danielsson & Tjøstheim 2004 |

| | | |
|---|---|---|
| Guidelines for preserving digital evidence, processes, procedures, and suggestions to use technologies | Dimension | Danielsson & Tjøstheim 2004 |
| Assets and customers | Dimension | Danielsson & Tjøstheim 2004 |
| Forensic policies | Dimension | Wolfe 2004 |
| Chain of evidence | Dimension | Wolfe 2004 |
| Develop a strategy to prepare the underlying systems from a forensic viewpoint | Dimension | Casey 2005 |
| Case management and incident tracking | Dimension | Casey 2005 |
| Laboratory accreditation and auditing | Dimension | Chen, Tsai, Chen & Yee 2005 |
| A quality assurance system that covers quality policies, activities, procedures, documentation, and management. | Dimension | Chen, Tsai, Chen & Yee 2005 |
| Procedures to control the quality of documents | Dimension | Chen, Tsai, Chen & Yee 2005 |
| Archive Management | Dimension | Chen, Tsai, Chen & Yee 2005 |
| Forensic knowledge of IT management | Dimension | Quinn 2005 |
| Policies and procedures | Dimension | Quinn 2005 |
| What are the skills and abilities of the computer forensic examiners? | Dimension | Rogers, Goldman, Mislan, Wedge & Debrota 2006 |
| What type of technology is involved (standalone systems, complex networks etc.)? | Dimension | Rogers, Goldman, Mislan, Wedge & Debrota 2006 |
| Maintaining the integrity of digital evidence | Dimension | Rogers, Goldman, Mislan, Wedge & Debrota 2006 |
| Maintaining the chain of custody of evidence | Dimension | Rogers, Goldman, Mislan, Wedge & Debrota 2006 |
| Complying with rules of evidence for admissibility at the Federal and State levels | Dimension | Rogers, Goldman, Mislan, Wedge & Debrota 2006 |
| Planning and pre-raid intelligence | Dimension | Rogers, Goldman, Mislan, Wedge & Debrota 2006 |
| Policies including contacting law enforcement, performing monitoring, and conducting regular reviews of forensic policies and procedures | Dimension | Kent, Chevalier, Grance & Dang 2006 |
| Procedures and guidelines for performing forensic tasks,based on the organization's policies and all applicable laws and regulations | Dimension | Kent, Chevalier, Grance & Dang 2006 |
| Policies and procedures supporting reasonable and appropriate use of forensic tools | Dimension | Kent, Chevalier, Grance & Dang 2006 |
| Demonstrate conclusively the authenticity, credibility, and reliability of electronic records | Dimension | Kent, Chevalier, Grance & Dang 2006 |
| Capability to perform computer and network forensics | Dimension | Kent, Chevalier, Grance & Dang 2006 |
| 1. What are the potential sources of data? | Dimension | Kent, Chevalier, Grance & Dang 2006 |
| 4. Which forensic tools and techniques would most likely be used? Which other tools and techniques might also be used? | Dimension | Kent, Chevalier, Grance & Dang 2006 |

| | | |
|---|---|---|
| 5. Which groups and individuals within the organization would probably be involved in the forensic activities? | Dimension | Kent, Chevalier, Grance & Dang 2006 |
| 6. What communications with external parties might occur, if any? | Dimension | Kent, Chevalier, Grance & Dang 2006 |
| Information Management Team including experts in computer forensics, law, information management, information technology, and auditing | Dimension | Luoma 2006 |
| Electronic document retention and deletion policy | Dimension | Luoma 2006 |
| Employees knowledge on information management and awareness of policies | Dimension | Luoma 2006 |
| Planning Information Retention Requirements | Dimension | VonSolms, Lowurens, Reeky & Grobler 2006 |
| Gather potential evidence | Dimension | VonSolms, Lowurens, Reeky & Grobler 2006 |
| Prevent anonymous activities | Dimension | VonSolms, Lowurens, Reeky & Grobler 2006 |
| Planning the response. | Dimension | VonSolms, Lowurens, Reeky & Grobler 2006 |
| Digital Forensic Training | Dimension | VonSolms, Lowurens, Reeky & Grobler 2006 |
| Accelerating the DF investigation. | Dimension | VonSolms, Lowurens, Reeky & Grobler 2006 |
| Incident response team | Dimension | Forrester & Irwin 2007 |
| Organisational policies and procedures | Dimension | Forrester & Irwin 2007 |
| Pre-emptive systems in place | Dimension | Forrester & Irwin 2007 |
| Corporate governance material converted into a Forensic Readiness Policy | Dimension | Forrester & Irwin 2007 |
| Legal context | Dimension | Forrester & Irwin 2007 |
| Good corporate governance, specifically IS governance | Dimension | Grobler & Louwrens 2007 |
| Use of DF tools | Dimension | Grobler & Louwrens 2007 |
| IS and DF awareness training | Dimension | Grobler & Louwrens 2007 |
| IS and DF policies | Dimension | Grobler & Louwrens 2007 |
| Establish a capability to securely gather admissible evidence by considering technology and human capacity | Dimension | Grobler & Louwrens 2007 |
| Developing a preservation culture in the organization to preserve all processes and activities should an investigation arise; | Dimension | Grobler & Louwrens 2007 |
| Establishment of policies in terms of digital assets, forensic events, data collection and storage | Dimension | Taylor, Endicott-Popovsky & Frincke 2007 |
| Multidisciplinary approach (Law, IT, Enforcement, Business) | Dimension | Bem, Feld, Huebner & Bem 2008 |
| Computer Security Incident Response Teams (CSIRTs) | Dimension | Khurana, Basney, Bakht, Freemon, Welch & Butler 2009 |
| Digital investigation procedures | Dimension | Khurana, Basney, Bakht, Freemon, Welch & Butler 2009 |
| Interaction with law enforcement | Dimension | Khurana, Basney, Bakht, Freemon, Welch & Butler 2009 |

| | | |
|---|---|---|
| Emergency Response Teams (CERTs) | Dimension | Khurana, Basney, Bakht, Freemon, Welch & Butler 2009 |
| Analysis of logs and alerts gathered by IDSs, server logs, and network logs | Dimension | Khurana, Basney, Bakht, Freemon, Welch & Butler 2009 |
| Roles and Responsibilities Model | Dimension | Khurana, Basney, Bakht, Freemon, Welch & Butler 2009 |
| Plethora of useful tools (IDS, Centralized logging) | Dimension | Khurana, Basney, Bakht, Freemon, Welch & Butler 2009 |
| Site Technical Roles (Lead, Incident Investigator, Digital Forensics Specialist, Security/System Administrator, Security/System Architect) | Dimension | Khurana, Basney, Bakht, Freemon, Welch & Butler 2009 |
| Collaboration Technical Roles (Lead, Incident Investigator, Digital Forensics Specialist, Workspace Administrator) | Dimension | Khurana, Basney, Bakht, Freemon, Welch & Butler 2009 |
| Site Legal Roles (Legal Adviser, Liason with Law Enforcement) | Dimension | Khurana, Basney, Bakht, Freemon, Welch & Butler 2009 |
| Law Enforcement Roles (Prosecutor, Investigator, Executive, Media Liason) | Dimension | Khurana, Basney, Bakht, Freemon, Welch & Butler 2009 |
| Preparation of security system architecture documentation | Dimension | Khurana, Basney, Bakht, Freemon, Welch & Butler 2009 |
| Train staff on latest threats and software tools | Dimension | Khurana, Basney, Bakht, Freemon, Welch & Butler 2009 |
| Deploy intrusion detection and forensics data collection capabilities | Dimension | Khurana, Basney, Bakht, Freemon, Welch & Butler 2009 |
| Develop incident response policies, procedures and legal coordination plan | Dimension | Khurana, Basney, Bakht, Freemon, Welch & Butler 2009 |
| Establish and maintain a collaborative workspace hosting environment | Dimension | Khurana, Basney, Bakht, Freemon, Welch & Butler 2009 |
| Develop/deploy collaborative tools, policies and procedures | Dimension | Khurana, Basney, Bakht, Freemon, Welch & Butler 2009 |
| Chain of custody | Dimension | Khurana, Basney, Bakht, Freemon, Welch & Butler 2009 |
| ID Management | Dimension | Dlamini, Eloff, & Eloff 2009 |
| Information Security Management | Dimension | Dlamini, Eloff, & Eloff 2009 |
| Legal & Regulatory Compliance | Dimension | Dlamini, Eloff, & Eloff 2009 |
| Network Security | Dimension | Dlamini, Eloff, & Eloff 2009 |
| Physical Security | Dimension | Dlamini, Eloff, & Eloff 2009 |
| Privacy | Dimension | Dlamini, Eloff, & Eloff 2009 |
| Risk Management | Dimension | Dlamini, Eloff, & Eloff 2009 |
| Software Security | Dimension | Dlamini, Eloff, & Eloff 2009 |
| Wireless infrastructure security | Dimension | Dlamini, Eloff, & Eloff 2009 |
| Internal network security | Dimension | Dlamini, Eloff, & Eloff 2009 |
| Management involvement, risk management | Dimension | Dlamini, Eloff, & Eloff 2009 |
| User education, training and awareness | Dimension | Dlamini, Eloff, & Eloff 2009 |
| Policy & regulatory compliance (Sarbanes–Oxley, HIPAA) | Dimension | Dlamini, Eloff, & Eloff 2009 |
| Data protection | Dimension | Dlamini, Eloff, & Eloff 2009 |
| An overall forensic policy | Dimension | Reddy & Venter 2009 |
| Technical readiness procedures and processes | Dimension | Reddy & Venter 2009 |

| | | |
|---|---|---|
| Non-technical readiness procedures and processes | Dimension | Reddy & Venter 2009 |
| Monitoring and auditing | Dimension | Reddy & Venter 2009 |
| Hardware and software configured properly | Dimension | Reddy & Venter 2009 |
| Education of forensic team members and appropriate certifications | Dimension | Reddy & Venter 2009 |
| Architecture | Dimension | Reddy & Venter 2009 |
| Legal limitations | Dimension | Garfinkel 2010 |
| Mobile computing | Dimension | Garfinkel 2010 |
| Training | Dimension | Garfinkel 2010 |
| International laws | Dimension | Garfinkel 2010 |
| Functionality of DF tools | Dimension | Garfinkel 2010 |
| Collaboration | Dimension | Garfinkel 2010 |
| Strategy | Dimension | Barske, Stander & Jordaan 2010 |
| Compliance & Monitoring | Dimension | Barske, Stander & Jordaan 2010 |
| Policy & Procedures | Dimension | Barske, Stander & Jordaan 2010 |
| Technology | Dimension | Barske, Stander & Jordaan 2010 |
| Digital Forensic Response | Dimension | Barske, Stander & Jordaan 2010 |
| Staff IT skills | Dimension | Barske, Stander & Jordaan 2010 |
| Chain of custody is kept for the evidence | Dimension | Barske, Stander & Jordaan 2010 |
| Quality assurance to ensure that the examination and analysis | Dimension | Barske, Stander & Jordaan 2010 |
| Policy, people and process adaptation to DF | Dimension | Barske, Stander & Jordaan 2010 |
| Updating the organisation’s policies and procedures | Dimension | Barske, Stander & Jordaan 2010 |
| The systematic gathering of potential digital evidence | Dimension | Barske, Stander & Jordaan 2010 |
| The secure storage of potential digital evidence | Dimension | Barske, Stander & Jordaan 2010 |
| Preparation for events requiring digital forensic intervention | Dimension | Barske, Stander & Jordaan 2010 |
| Enhanced capability for evidence retrieval | Dimension | Barske, Stander & Jordaan 2010 |
| Legal advice | Dimension | Barske, Stander & Jordaan 2010 |
| Developing of an in-house digital forensics examination and analysis capacity | Dimension | Barske, Stander & Jordaan 2010 |
| Identifying and understanding retention records legislation | Dimension | Barske, Stander & Jordaan 2010 |
| Computers and Servers | Dimension | Barske, Stander & Jordaan 2010 |
| Acquisition and Analysis technology | Dimension | Barske, Stander & Jordaan 2010 |
| Evidence Storage technology | Dimension | Barske, Stander & Jordaan 2010 |
| Interdisciplinary formal programs to educate professionals | Dimension | Duranti & Endicott-Popovsky 2010 |
| Infrastructure preparedness | Dimension | Grobler, Louwrens & Von Solms 2010 |
| Existance of risk mitigation plans including evidence and process requirements | Dimension | Grobler, Louwrens & Von Solms 2010 |
| Preparation for containments of incidents to include containment on live systems | Dimension | Grobler, Louwrens & Von Solms 2010 |

| | | |
|---|---|---|
| Use of IT tools | Dimension | Grobler, Louwrens & Von Solms 2010 |
| Minimization of business interruption | Dimension | Grobler, Louwrens & Von Solms 2010 |
| Efficiency | Dimension | Grobler, Louwrens & Von Solms 2010 |
| Specific requirements per country, jurisdiction, and industry for admissible evidence | Dimension | Grobler, Louwrens & Von Solms 2010 |
| Ability to prove compliance | Dimension | Grobler, Louwrens & Von Solms 2010 |
| Active DF capabilities in live system environments | Dimension | Grobler, Louwrens & Von Solms 2010 |
| Establishment of policies and procedures | Dimension | Grobler, Louwrens & Von Solms 2010 (2) |
| Legal | Dimension | Grobler, Louwrens & Von Solms 2010 (2) |
| Policies | Dimension | Grobler, Louwrens & Von Solms 2010 (2) |
| Governance | Dimension | Grobler, Louwrens & Von Solms 2010 (2) |
| People | Dimension | Grobler, Louwrens & Von Solms 2010 (2) |
| Process | Dimension | Grobler, Louwrens & Von Solms 2010 (2) |
| Technology | Dimension | Grobler, Louwrens & Von Solms 2010 (2) |
| Implemented processes and methodologies | Dimension | Hoolachan & Glisson 2010 |
| Legal aspects | Dimension | Hoolachan & Glisson 2010 |
| The individuals involved in the investigation | Dimension | Hoolachan & Glisson 2010 |
| Business aspects | Dimension | Hoolachan & Glisson 2010 |
| Social aspects | Dimension | Hoolachan & Glisson 2010 |
| Technical aspects | Dimension | Hoolachan & Glisson 2010 |
| Legal apects e.g. admissibility and jurisdiction | Dimension | Hoolachan & Glisson 2010 |
| Security training | Dimension | Hoolachan & Glisson 2010 |
| Organizational culture | Dimension | Hoolachan & Glisson 2010 |
| Monitoring | Dimension | Ngobeni, Venter & Burke 2010 |
| Logging | Dimension | Ngobeni, Venter & Burke 2010 |
| Preservation | Dimension | Ngobeni, Venter & Burke 2010 |
| Analysis | Dimension | Ngobeni, Venter & Burke 2010 |
| Report | Dimension | Ngobeni, Venter & Burke 2010 |
| Cloud computing | Dimension | Taylor, Haggerty, Gresty & Hegarty 2010 |
| Jurisdictional difficulties | Dimension | Taylor, Haggerty, Gresty & Hegarty 2010 |
| Encryption | Dimension | Taylor, Haggerty, Gresty & Hegarty 2010 |
| Resourcing of the incident response capability | Dimension | Shedden, Ahmad & Ruighaver 2010 |
| Availability and application of technical expertise | Dimension | Shedden, Ahmad & Ruighaver 2010 |
| Organizational skill in creating, acquiring | Dimension | Shedden, Ahmad & Ruighaver 2010 |

| | | |
|---|---|---|
| and transfering knowledge | | |
| Corporate security policies | Dimension | Pangalos, Ilioudis & Pagkalos 2010 |
| Law framework | Dimension | Pangalos, Ilioudis & Pagkalos 2010 |
| Security policy | Dimension | Pangalos, Ilioudis & Pagkalos 2010 |
| The scene, the requirements, the methodology and tools used, the results and reports | Dimension | Pangalos, Ilioudis & Pagkalos 2010 |
| Processes related to data backup and recovery | Dimension | Pangalos, Ilioudis & Pagkalos 2010 |
| Encryption | Dimension | Taylor, Haggerty, Gresty & Lamb 2011 |
| 9. Implementing defined procedures and PKI system architecture | Dimension | Valjarevic & Venter 2011 |
| Organizational policy which will consider the preventative side of security | Dimension | Mouhtaropoulos, Grobler & Li 2011 |
| Control to DE access and maintenance of a digital chain of custody (DCOC). | Dimension | Mouhtaropoulos, Grobler & Li 2011 |
| Evidence Management Plan development | Dimension | Mouhtaropoulos, Grobler & Li 2011 |
| Technical infrastructure standards. | Dimension | Mouhtaropoulos, Grobler & Li 2011 |
| Ability to collect the evidence without disrupting the environment. | Dimension | Mouton & Venter 2011 |
| Privacy | Dimension | Spyridopoulos & Katos 2011 |
| Jurisdiction | Dimension | Spyridopoulos & Katos 2011 |
| Cloud storage | Dimension | Spyridopoulos & Katos 2011 |
| Legal procedure | Dimension | Spyridopoulos & Katos 2011 |
| Organisational resources coordination | Dimension | Reddy, Venter & Olivier 2012 |
| Development of IT infrastructure | Dimension | Reddy, Venter & Olivier 2012 |
| IT security and DF programmes maturity | Dimension | Reddy, Venter & Olivier 2012 |
| Legal requirements | Dimension | Leigh 2012 |
| IT systems in use. | Dimension | Leigh 2012 |
| Back-up procedures. | Dimension | Leigh 2012 |
| Electronic document retention and archiving policies. | Dimension | Leigh 2012 |
| Employment law or privacy issues | Dimension | Leigh 2012 |
| Likely threats | Dimension | Hamidovic 2012 |
| How to secure data | Dimension | Hamidovic 2012 |
| Legal problems (e.g. admissibility, data protection, human rights, limits to surveillance, obligations to staff members and others, and disclosure in legal proceedings) | Dimension | Hamidovic 2012 |
| Management, skill, and resource implications and developed an action plan | Dimension | Hamidovic 2012 |
| Information retention | Dimension | Pooe & Labuschagne 2012 |
| Response planning | Dimension | Pooe & Labuschagne 2012 |
| Training | Dimension | Pooe & Labuschagne 2012 |
| Investigation acceleration | Dimension | Pooe & Labuschagne 2012 |
| Evidence protection | Dimension | Pooe & Labuschagne 2012 |
| People | Dimension | Pooe & Labuschagne 2012 |

| | | |
|---|---|---|
| Process | Dimension | Pooe & Labuschagne 2012 |
| Policy | Dimension | Pooe & Labuschagne 2012 |
| Technology | Dimension | Pooe & Labuschagne 2012 |
| Computer Incident response Team (CIRT) information and skills management | Dimension | Pooe & Labuschagne 2012 |
| Security awareness | Dimension | Pooe & Labuschagne 2012 |
| Planning of incident response | Dimension | Pooe & Labuschagne 2012 |
| Storage technology | Dimension | Pooe & Labuschagne 2012 |
| Policies & Procedures | Dimension | Pooe & Labuschagne 2012 |
| Incident Management | Dimension | Pooe & Labuschagne 2012 |
| Management commitment and leadership to secure information systems | Dimension | Elachgar, Boulafdour, Makoudi & Regragui 2012 |
| User awareness of the issues, threats and best practices in information security | Dimension | Elachgar, Boulafdour, Makoudi & Regragui 2012 |
| The implementation of policies, processes and procedures to secure the information system | Dimension | Elachgar, Boulafdour, Makoudi & Regragui 2012 |
| Adequate technology to secure the information system | Dimension | Elachgar, Boulafdour, Makoudi & Regragui 2012 |
| Compliance with regulatory requirements according to information security information | Dimension | Elachgar, Boulafdour, Makoudi & Regragui 2012 |
| Risk analysis | Dimension | Elachgar, Boulafdour, Makoudi & Regragui 2012 |
| Security indicators | Dimension | Elachgar, Boulafdour, Makoudi & Regragui 2012 |
| Security of premises | Dimension | Elachgar, Boulafdour, Makoudi & Regragui 2012 |
| Architecture and Systems Security | Dimension | Elachgar, Boulafdour, Makoudi & Regragui 2012 |
| Development of action plans | Dimension | Elachgar, Boulafdour, Makoudi & Regragui 2012 |
| Records management including the cloud | Dimension | Ferguson-Boucher & Endicott-Popovsky 2012 |
| Information governance and assurance (confidentiality, integrity, availability, authentication and non-repudiation) | Dimension | Ferguson-Boucher & Endicott-Popovsky 2012 |
| Chain of custody is kept for the evidence | Dimension | Ferguson-Boucher & Endicott-Popovsky 2012 |
| Cross-disciplinary teams | Dimension | Ferguson-Boucher & Endicott-Popovsky 2012 |
| The preservation, continuity, mainainability and resilience of cloud information | Dimension | Ferguson-Boucher & Endicott-Popovsky 2012 |
| Cloud warehousing | Dimension | Ferguson-Boucher & Endicott-Popovsky 2012 |
| Legal framework and jurisdictions | Dimension | Ferguson-Boucher & Endicott-Popovsky 2012 |
| Generally accepted standardized training and certification programs | Dimension | Mouhtaropoulos & Li 2012 |
| Policies from yasinsac & Manzano | Dimension | Mouhtaropoulos & Li 2012 |
| Risk assessment | Dimension | Mouhtaropoulos & Li 2012 |
| Data identification | Dimension | Mouhtaropoulos & Li 2012 |

|  |  |  |
|---|---|---|
| Forensic policy writing and Legal review | Dimension | Mouhtaropoulos & Li 2012 |
| Digital evidence management | Dimension | Mouhtaropoulos & Li 2012 |
| Incident response process | Dimension | Mouhtaropoulos & Li 2012 |
| Staff training | Dimension | Mouhtaropoulos & Li 2012 |
| Depict results on a Cost-Benefit factor relation model | Dimension | Mouhtaropoulos & Li 2012 |
| Risk Assessment | Dimension | Mouhtaropoulos, Dimotikalis & Li 2013 |
| Digital Evidence Management | Dimension | Mouhtaropoulos, Dimotikalis & Li 2013 |
| Staff Training | Dimension | Mouhtaropoulos, Dimotikalis & Li 2013 |
| Incident Response Process | Dimension | Mouhtaropoulos, Dimotikalis & Li 2013 |
| Policies & Procedures | Dimension | Mouhtaropoulos, Dimotikalis & Li 2013 |
| Business Scenarios | Dimension | Mouhtaropoulos, Dimotikalis & Li 2013 |
| Digital Evidence Preparation | Dimension | Mouhtaropoulos, Dimotikalis & Li 2013 |
| Human factor | Dimension | Mouhtaropoulos, Dimotikalis & Li 2013 |
| Specific methodology to capture, stored, analyze, preserve, integrate, present evidence | Dimension | Mouhtaropoulos, Li & Grobler 2012 |
| Relevant software tools to capture, stored, analyze, preserve, integrate, present evidence | Dimension | Mouhtaropoulos, Li & Grobler 2012 |
| Risk assessment analysis | Dimension | Mouhtaropoulos, Li & Grobler 2012 |
| Event analysis | Dimension | Reddy & Venter 2013 |
| DFR information | Dimension | Reddy & Venter 2013 |
| Costing | Dimension | Reddy & Venter 2013 |
| Staff from multiple departments and business units | Dimension | Reddy & Venter 2013 |
| Network infrastructure and computing platforms | Dimension | Reddy & Venter 2013 |
| Investigative teams (DF teams) and incident response teams descriptions | Dimension | Reddy & Venter 2013 |
| Training requirements and training | Dimension | Reddy & Venter 2013 |
| Business process descriptions | Dimension | Reddy & Venter 2013 |
| Organisational DF policies and policies related to DFR | Dimension | Reddy & Venter 2013 |
| Incident response procedure | Dimension | Reddy & Venter 2013 |
| Defined organisational structure, privileges and rank hierarchy | Dimension | Reddy & Venter 2013 |
| Staff involved in DFR and incident response | Dimension | Reddy & Venter 2013 |
| Storage of information about training, procedures, people, roles, policies, etc. | Dimension | Reddy & Venter 2013 |
| Documentation of incidents and investigation archive | Dimension | Reddy & Venter 2013 |
| Network forensics | Dimension | Sibiya, Venter & Ngobeni 2013 |
| Computer forensics | Dimension | Sibiya, Venter & Ngobeni 2013 |
| Data and Process provenance | Dimension | Trenwith & Venter 2013 |
| Integrity of the evidence and chain of custody | Dimension | Trenwith & Venter 2013 |
| Jurisdictional issues | Dimension | Trenwith & Venter 2013 |

| | | |
|---|---|---|
| Cloudification | Dimension | Trenwith & Venter 2013 |
| Encryption | Dimension | Trenwith & Venter 2013 |
| Qualified individuals | Dimension | Elyas, Maynard, Ahmad & Lonie 2014 |
| Forensic strategy | Dimension | Elyas, Maynard, Ahmad & Lonie 2014 |
| Non-technical stakeholders | Dimension | Elyas, Maynard, Ahmad & Lonie 2014 |
| Technical stakeholders | Dimension | Elyas, Maynard, Ahmad & Lonie 2014 |
| Technology | Dimension | Elyas, Maynard, Ahmad & Lonie 2014 |
| Monitoring | Dimension | Elyas, Maynard, Ahmad & Lonie 2014 |
| Architecture | Dimension | Elyas, Maynard, Ahmad & Lonie 2014 |
| Policies | Dimension | Elyas, Maynard, Ahmad & Lonie 2014 |
| Training | Dimension | Elyas, Maynard, Ahmad & Lonie 2014 |
| Forensic culture | Dimension | Elyas, Maynard, Ahmad & Lonie 2014 |
| Governance | Dimension | Elyas, Maynard, Ahmad & Lonie 2014 |
| Encryption | Dimension | Elyas, Maynard, Ahmad & Lonie 2014 |
| Communications with external stakeholders | Dimension | Elyas, Maynard, Ahmad & Lonie 2014 |
| Appropriate organizational structure that takes forensics into account | Dimension | Elyas, Maynard, Ahmad & Lonie 2014 |
| Staff awareness | Dimension | Elyas, Maynard, Ahmad & Lonie 2014 |
| Capabilities of legal evidence management | Dimension | Elyas, Maynard, Ahmad & Lonie 2014 |
| Capabilities of internal investigations | Dimension | Elyas, Maynard, Ahmad & Lonie 2014 |
| Capabilities of regulatory compliance | Dimension | Elyas, Maynard, Ahmad & Lonie 2014 |
| Security awareness | Dimension | Web, Ahmad, Maynard / Shanks 2014 |
| Personnel understand the technology | Dimension | Web, Ahmad, Maynard / Shanks 2014 |
| Objective of DFR program e.g. business objectives, compliance, internal investigation, forensic response, and legal evidence management | Dimension | Elyas, Ahmad, Maynard & Lonie 2015 |
| Organizational Factors (Top Management Support, Governance, Culture) Elyas 2014 | Dimension | Elyas, Ahmad, Maynard & Lonie 2015 |
| Validated forensic tools | Dimension | Elyas, Ahmad, Maynard & Lonie 2015 |
| Maintenance and testing of systems | Dimension | Elyas, Ahmad, Maynard & Lonie 2015 |
| Resourcing | Dimension | Elyas, Ahmad, Maynard & Lonie 2015 |
| Technology use and selection | Dimension | Elyas, Ahmad, Maynard & Lonie 2015 |
| Forensic Training | Dimension | Elyas, Ahmad, Maynard & Lonie 2015 |
| Policy | Dimension | Elyas, Ahmad, Maynard & Lonie 2015 |
| Organisational structure that takes forensics into consideration | Dimension | Elyas, Ahmad, Maynard & Lonie 2015 |

# APPENDIX C - Q-SORT TEST SURVEY

## DFR Dimensions Survey

Q1 Thanks for your participation in this study. By accepting to take this survey you consent with the utilization of this information for the purpose of the study and acknowledge that your participation is voluntary. You can abandon this survey at any time. However, it is appreciated that you complete all required information to the best of your knowledge. This study has been reviewed by The University of Mississippi's Institutional Review Board (IRB). If you have any questions, concerns, or reports regarding your rights as a participant of research, please contact the IRB at (662) 915-7482 or irb@olemiss.edu.

Mark with an x:

○ Accept (1)
○ Decline (2)

Q2 What is your age range in years?

○ Below 18 (1)
○ 18 to 25 (2)
○ 26 to 33 (3)
○ 34 to 41 (4)
○ 42 to 49 (5)
○ 50 to 57 (6)
○ Above 57 (7)

Q3 What is your gender?

○ Male (1)
○ Female (2)

Q4 What is your experience with computer information systems in years?

○ Less than 1 (1)
○ 1 to 5 (2)
○ 6 to 10 (3)
○ 11 to 15 (4)
○ 16 to 20 (5)
○ 21 to 25 (6)
○ More than 25 (7)

Q5 What is your experience in information security in years?

○ Less than 1 (1)
○ 1 to 5 (2)
○ 6 to 10 (3)
○ 11 to 15 (4)
○ 16 to 20 (5)
○ 21 to 25 (6)
○ More than 25 (7)

Q6 What is your level of expertise in information security?

○ Layman (1)
○ Minimal (2)

○ Below average (3)
○ Average (4)
○ Above average (5)
○ Superior (6)
○ Expert (7)

Q7 Many factors affect the digital forensic readiness (DFR) of organizations. These factors can be classified in different categories or dimensions. Your task is to help determine these categories by grouping the following words into a set of minimal, unique and independent dimensions to which different factors of DFR might belong.

**Instructions**

Along with this document, you will find 65 tags that each contain a different word. These words might each indicate an independent category. However, some of them might belong to the same category because they are synonyms or because they together determine a theme that is independent of other categories proposed. It is your task to determine whether some of the words should be grouped or not.

An easy way to perform this task is to spread all the tags on a table and make clusters of words by placing together those which you believe belong together in a category, leaving alone those words that define a category by themselves. There is no limit for the number of words in a category or group. You might decide that each word is an independent category. However, the purpose of the exercise is to attempt to define the minimum number of categories possible.

Once your grouping is done, please place a rubber band (provided) around each bundle of two or more words making a category. Please, place the word that best represents the category on the top of the stack before placing the rubber band around it.

Count the total categories you defined and write it here: _____

If you feel that there may exist super-categories into which one or several rubber-band-bound collections and remaining single-words categories may be arranged, please place the grouped items together with another rubber band around all items within each super-category.

Count the total super-categories you defined and write it here: _____

Please, put all documents, the tied bundles of words and the loose words into the envelope provided and return it to the researcher.

Thanks for your time and effort.

# APPENDIX D - RESULT OF ASSOCIATION RULES FROM R

```
Apriori
Parameter specification:
Confidence: 0.5263
Minval: 0.1
Smax: 1
Arem: none
Aval: FALSE
OriginalSupport: TRUE
Support: 0.03968
Minlen: 2
Maxlen: 10
Target: rules
Ext: FALSE
Algorithmic control:
Filter: 0.1
Tree: TRUE
Heap: TRUE
Memopt: FALSE
Load: TRUE
Sort: 2
Verbose: TRUE
Absolute minimum support count: 9
set item appearances ...[0 item(s)] done [0.00s].
set transactions ...[65 item(s), 252 transaction(s)] done [0.00s].
sorting and recoding items ... [65 item(s)] done [0.00s].
creating transaction tree ... done [0.00s].
checking subsets of size 1 2 3 4 5 6 done [0.00s].
writing ... [403 rule(s)] done [0.00s].
creating S4 object  ... done [0.00s].
```

**Accepted Association Rules (Min. Support = 0.0397, Min. Confidence = 0.526)**

```
   lhs                                  rhs
support    confidence lift
1   {Stakeholder}                          => {People}         0.05952381 0.7894737  10.470914
2   {People}                             => {Stakeholder}    0.05952381 0.7894737  10.470914
3   {Stakeholder}                          => {User}          0.05952381 0.7894737  10.470914
4   {User}                             => {Stakeholder}    0.05952381 0.7894737  10.470914
5   {Stakeholder}                          => {Customer}       0.06349206 0.8421053  11.168975
6   {Customer}                            => {Stakeholder}    0.06349206 0.8421053  11.168975
7   {Stakeholder}                          => {Team}          0.04761905 0.6315789   8.376731
8   {Team}                               => {Stakeholder}    0.04761905 0.6315789   8.376731
9   {Stakeholder}                          => {Personnel}      0.05158730 0.6842105   9.074792
10  {Personnel}                           => {Stakeholder}    0.05158730 0.6842105   9.074792
11  {Threat}                             => {Risk}          0.06349206 0.8421053  11.168975
12  {Risk}                              => {Threat}        0.06349206 0.8421053  11.168975
13  {Threat}                             => {Intrusion}      0.05555556 0.7368421   9.772853
14  {Intrusion}                           => {Threat}        0.05555556 0.7368421   9.772853
15  {Threat}                             => {Attack}        0.05555556 0.7368421   9.772853
16  {Attack}                             => {Threat}        0.05555556 0.7368421   9.772853
17  {Threat}                             => {Target}        0.03968254 0.5263158   6.980609
```

```
18  {Target}        => {Threat}        0.03968254 0.5263158   6.980609
19  {People}        => {User}          0.06746032 0.8947368  11.867036
20  {User}          => {People}        0.06746032 0.8947368  11.867036
21  {People}        => {Customer}      0.06746032 0.8947368  11.867036
22  {Customer}      => {People}        0.06746032 0.8947368  11.867036
23  {People}        => {Team}          0.05555556 0.7368421   9.772853
24  {Team}          => {People}        0.05555556 0.7368421   9.772853
25  {People}        => {Personnel}     0.05555556 0.7368421   9.772853
26  {Personnel}     => {People}        0.05555556 0.7368421   9.772853
27  {Business}      => {Corporate}     0.06349206 0.8421053  11.168975
28  {Corporate}     => {Business}      0.06349206 0.8421053  11.168975
29  {Business}      => {Organization}  0.05952381 0.7894737  10.470914
30  {Organization}  => {Business}      0.05952381 0.7894737  10.470914
31  {User}          => {Customer}      0.07142857 0.9473684  12.565097
32  {Customer}      => {User}          0.07142857 0.9473684  12.565097
33  {User}          => {Team}          0.05158730 0.6842105   9.074792
34  {Team}          => {User}          0.05158730 0.6842105   9.074792
35  {User}          => {Personnel}     0.05555556 0.7368421   9.772853
36  {Personnel}     => {User}          0.05555556 0.7368421   9.772853
37  {Risk}          => {Intrusion}     0.04761905 0.6315789   8.376731
38  {Intrusion}     => {Risk}          0.04761905 0.6315789   8.376731
39  {Risk}          => {Attack}        0.04761905 0.6315789   8.376731
40  {Attack}        => {Risk}          0.04761905 0.6315789   8.376731
41  {Customer}      => {Team}          0.05158730 0.6842105   9.074792
42  {Team}          => {Customer}      0.05158730 0.6842105   9.074792
43  {Customer}      => {Personnel}     0.05555556 0.7368421   9.772853
44  {Personnel}     => {Customer}      0.05555556 0.7368421   9.772853
45  {Corporate}     => {Organization}  0.05158730 0.6842105   9.074792
46  {Organization}  => {Corporate}     0.05158730 0.6842105   9.074792
47  {Team}          => {Personnel}     0.05952381 0.7894737  10.470914
48  {Personnel}     => {Team}          0.05952381 0.7894737  10.470914
49  {Workspace}     => {Site}          0.04761905 0.6315789   8.376731
50  {Site}          => {Workspace}     0.04761905 0.6315789   8.376731
51  {Workspace}     => {Space}         0.05555556 0.7368421   9.772853
52  {Space}         => {Workspace}     0.05555556 0.7368421   9.772853
53  {Workspace}     => {Premises}      0.04761905 0.6315789   8.376731
54  {Premises}      => {Workspace}     0.04761905 0.6315789   8.376731
55  {Workspace}     => {Environment}   0.04761905 0.6315789   8.376731
56  {Environment}   => {Workspace}     0.04761905 0.6315789   8.376731
57  {Workspace}     => {Lab}           0.03968254 0.5263158   6.980609
58  {Lab}           => {Workspace}     0.03968254 0.5263158   6.980609
59  {Site}          => {Space}         0.03968254 0.5263158   6.980609
60  {Space}         => {Site}          0.03968254 0.5263158   6.980609
61  {Site}          => {Premises}      0.05158730 0.6842105   9.074792
62  {Premises}      => {Site}          0.05158730 0.6842105   9.074792
63  {Site}          => {Environment}   0.03968254 0.5263158   6.980609
64  {Environment}   => {Site}          0.03968254 0.5263158   6.980609
65  {Intrusion}     => {Attack}        0.07539683 1.0000000  13.263158
66  {Attack}        => {Intrusion}     0.07539683 1.0000000  13.263158
67  {Intrusion}     => {Event}         0.04365079 0.5789474   7.678670
68  {Event}         => {Intrusion}     0.04365079 0.5789474   7.678670
69  {Intrusion}     => {Incident}      0.05158730 0.6842105   9.074792
70  {Incident}      => {Intrusion}     0.05158730 0.6842105   9.074792
71  {Intrusion}     => {Target}        0.03968254 0.5263158   6.980609
72  {Target}        => {Intrusion}     0.03968254 0.5263158   6.980609
73  {Attack}        => {Event}         0.04365079 0.5789474   7.678670
```

```
74  {Event}                  => {Attack}         0.04365079 0.5789474   7.678670
75  {Attack}                 => {Incident}       0.05158730 0.6842105   9.074792
76  {Incident}               => {Attack}         0.05158730 0.6842105   9.074792
77  {Attack}                 => {Target}         0.03968254 0.5263158   6.980609
78  {Target}                 => {Attack}         0.03968254 0.5263158   6.980609
79  {Event}                  => {Incident}       0.05952381 0.7894737  10.470914
80  {Incident}               => {Event}          0.05952381 0.7894737  10.470914
81  {Space}                  => {Premises}       0.03968254 0.5263158   6.980609
82  {Premises}               => {Space}          0.03968254 0.5263158   6.980609
83  {Space}                  => {Environment}    0.04761905 0.6315789   8.376731
84  {Environment}            => {Space}          0.04761905 0.6315789   8.376731
85  {Record}                 => {Document}       0.03968254 0.5263158   6.980609
86  {Document}               => {Record}         0.03968254 0.5263158   6.980609
87  {Law}                    => {Rule}           0.04761905 0.6315789   8.376731
88  {Rule}                   => {Law}            0.04761905 0.6315789   8.376731
89  {Resource}               => {Asset}          0.05158730 0.6842105   9.074792
90  {Asset}                  => {Resource}       0.05158730 0.6842105   9.074792
91  {Evidence}               => {Proof}          0.06349206 0.8421053  11.168975
92  {Proof}                  => {Evidence}       0.06349206 0.8421053  11.168975
93  {Proof}                  => {Case}           0.03968254 0.5263158   6.980609
94  {Case}                   => {Proof}          0.03968254 0.5263158   6.980609
95  {Information}            => {Data}           0.06349206 0.8421053  11.168975
96  {Data}                   => {Information}    0.06349206 0.8421053  11.168975
97  {System}                 => {Software}       0.03968254 0.5263158   6.980609
98  {Software}               => {System}         0.03968254 0.5263158   6.980609
99  {Requirement}            => {Policy}         0.03968254 0.5263158   6.980609
100 {Policy}                 => {Requirement}    0.03968254 0.5263158   6.980609
101 {Operation}              => {Process}        0.05555556 0.7368421   9.772853
102 {Process}                => {Operation}      0.05555556 0.7368421   9.772853
103 {Equipment}              => {Server}         0.05555556 0.7368421   9.772853
104 {Server}                 => {Equipment}      0.05555556 0.7368421   9.772853
105 {Equipment}              => {Network}        0.03968254 0.5263158   6.980609
106 {Network}                => {Equipment}      0.03968254 0.5263158   6.980609
107 {Equipment}              => {Hardware}       0.06349206 0.8421053  11.168975
108 {Hardware}               => {Equipment}      0.06349206 0.8421053  11.168975
109 {Equipment}              => {Computer}       0.05555556 0.7368421   9.772853
110 {Computer}               => {Equipment}      0.05555556 0.7368421   9.772853
111 {Program}                => {Software}       0.05158730 0.6842105   9.074792
112 {Software}               => {Program}        0.05158730 0.6842105   9.074792
113 {Program}                => {Code}           0.05555556 0.7368421   9.772853
114 {Code}                   => {Program}        0.05555556 0.7368421   9.772853
115 {Rule}                   => {Policy}         0.05158730 0.6842105   9.074792
116 {Policy}                 => {Rule}           0.05158730 0.6842105   9.074792
117 {Rule}                   => {Guideline}      0.04365079 0.5789474   7.678670
118 {Guideline}              => {Rule}           0.04365079 0.5789474   7.678670
119 {Objective}              => {Strategy}       0.03968254 0.5263158   6.980609
120 {Strategy}               => {Objective}      0.03968254 0.5263158   6.980609
121 {Software}               => {Code}           0.05158730 0.6842105   9.074792
122 {Code}                   => {Software}       0.05158730 0.6842105   9.074792
123 {Plan}                   => {Guideline}      0.04365079 0.5789474   7.678670
124 {Guideline}              => {Plan}           0.04365079 0.5789474   7.678670
125 {Plan}                   => {Strategy}       0.05952381 0.7894737  10.470914
126 {Strategy}               => {Plan}           0.05952381 0.7894737  10.470914
127 {Architecture}           => {Infrastructure} 0.04365079 0.5789474   7.678670
128 {Infrastructure}         => {Architecture}   0.04365079 0.5789474   7.678670
129 {Policy}                 => {Guideline}      0.05158730 0.6842105   9.074792
```

```
130 {Guideline}                  => {Policy}        0.05158730 0.6842105   9.074792
131 {Policy}                     => {Procedure}     0.03968254 0.5263158   6.980609
132 {Procedure}                  => {Policy}        0.03968254 0.5263158   6.980609
133 {Process}                    => {Flow}          0.03968254 0.5263158   6.980609
134 {Flow}                       => {Process}       0.03968254 0.5263158   6.980609
135 {Process}                    => {Procedure}     0.04761905 0.6315789   8.376731
136 {Procedure}                  => {Process}       0.04761905 0.6315789   8.376731
137 {Technology}                 => {Computer}      0.03968254 0.5263158   6.980609
138 {Computer}                   => {Technology}    0.03968254 0.5263158   6.980609
139 {Server}                     => {Network}       0.04761905 0.6315789   8.376731
140 {Network}                    => {Server}        0.04761905 0.6315789   8.376731
141 {Server}                     => {Hardware}      0.06349206 0.8421053  11.168975
142 {Hardware}                   => {Server}        0.06349206 0.8421053  11.168975
143 {Server}                     => {Computer}      0.05952381 0.7894737  10.470914
144 {Computer}                   => {Server}        0.05952381 0.7894737  10.470914
145 {Guideline}                  => {Strategy}      0.03968254 0.5263158   6.980609
146 {Strategy}                   => {Guideline}     0.03968254 0.5263158   6.980609
147 {Guideline}                  => {Procedure}     0.04365079 0.5789474   7.678670
148 {Procedure}                  => {Guideline}     0.04365079 0.5789474   7.678670
149 {Network}                    => {Hardware}      0.04761905 0.6315789   8.376731
150 {Hardware}                   => {Network}       0.04761905 0.6315789   8.376731
151 {Network}                    => {Computer}      0.04365079 0.5789474   7.678670
152 {Computer}                   => {Network}       0.04365079 0.5789474   7.678670
153 {Hardware}                   => {Computer}      0.06349206 0.8421053  11.168975
154 {Computer}                   => {Hardware}      0.06349206 0.8421053  11.168975
155 {Method}                     => {Procedure}     0.03968254 0.5263158   6.980609
156 {Procedure}                  => {Method}        0.03968254 0.5263158   6.980609
157 {People,Stakeholder}         => {User}          0.05952381 1.0000000  13.263158
158 {Stakeholder,User}           => {People}        0.05952381 1.0000000  13.263158
159 {People,User}                => {Stakeholder}   0.05952381 0.8823529  11.702786
160 {People,Stakeholder}         => {Customer}      0.05952381 1.0000000  13.263158
161 {Customer,Stakeholder}       => {People}        0.05952381 0.9375000  12.434211
162 {Customer,People}            => {Stakeholder}   0.05952381 0.8823529  11.702786
163 {People,Stakeholder}         => {Team}          0.04761905 0.8000000  10.610526
164 {Stakeholder,Team}           => {People}        0.04761905 1.0000000  13.263158
165 {People,Team}                => {Stakeholder}   0.04761905 0.8571429  11.368421
166 {People,Stakeholder}         => {Personnel}     0.05158730 0.8666667  11.494737
167 {Personnel,Stakeholder}      => {People}        0.05158730 1.0000000  13.263158
168 {People,Personnel}          => {Stakeholder}   0.05158730 0.9285714  12.315789
169 {Stakeholder,User}           => {Customer}      0.05952381 1.0000000  13.263158
170 {Customer,Stakeholder}       => {User}          0.05952381 0.9375000  12.434211
171 {Customer,User}              => {Stakeholder}   0.05952381 0.8333333  11.052632
172 {Stakeholder,User}           => {Team}          0.04761905 0.8000000  10.610526
173 {Stakeholder,Team}           => {User}          0.04761905 1.0000000  13.263158
174 {Team,User}                  => {Stakeholder}   0.04761905 0.9230769  12.242915
175 {Stakeholder,User}           => {Personnel}     0.05158730 0.8666667  11.494737
176 {Personnel,Stakeholder}      => {User}          0.05158730 1.0000000  13.263158
177 {Personnel,User}             => {Stakeholder}   0.05158730 0.9285714  12.315789
178 {Customer,Stakeholder}       => {Team}          0.04761905 0.7500000   9.947368
179 {Stakeholder,Team}           => {Customer}      0.04761905 1.0000000  13.263158
180 {Customer,Team}              => {Stakeholder}   0.04761905 0.9230769  12.242915
181 {Customer,Stakeholder}       => {Personnel}     0.05158730 0.8125000  10.776316
182 {Personnel,Stakeholder}      => {Customer}      0.05158730 1.0000000  13.263158
183 {Customer,Personnel}         => {Stakeholder}   0.05158730 0.9285714  12.315789
184 {Stakeholder,Team}           => {Personnel}     0.04365079 0.9166667  12.157895
185 {Personnel,Stakeholder}      => {Team}          0.04365079 0.8461538  11.222672
```

```
186 {Personnel,Team}             => {Stakeholder}   0.04365079 0.7333333   9.726316
187 {Risk,Threat}                => {Intrusion}     0.04761905 0.7500000   9.947368
188 {Intrusion,Threat}           => {Risk}          0.04761905 0.8571429  11.368421
189 {Intrusion,Risk}             => {Threat}        0.04761905 1.0000000  13.263158
190 {Risk,Threat}                => {Attack}        0.04761905 0.7500000   9.947368
191 {Attack,Threat}              => {Risk}          0.04761905 0.8571429  11.368421
192 {Attack,Risk}                => {Threat}        0.04761905 1.0000000  13.263158
193 {Intrusion,Threat}           => {Attack}        0.05555556 1.0000000  13.263158
194 {Attack,Threat}              => {Intrusion}     0.05555556 1.0000000  13.263158
195 {Attack,Intrusion}           => {Threat}        0.05555556 0.7368421   9.772853
196 {People,User}                => {Customer}      0.06746032 1.0000000  13.263158
197 {Customer,People}            => {User}          0.06746032 1.0000000  13.263158
198 {Customer,User}              => {People}        0.06746032 0.9444444  12.526316
199 {People,User}                => {Team}          0.05158730 0.7647059  10.142415
200 {People,Team}                => {User}          0.05158730 0.9285714  12.315789
201 {Team,User}                  => {People}        0.05158730 1.0000000  13.263158
202 {People,User}                => {Personnel}     0.05555556 0.8235294  10.922601
203 {People,Personnel}           => {User}          0.05555556 1.0000000  13.263158
204 {Personnel,User}             => {People}        0.05555556 1.0000000  13.263158
205 {Customer,People}            => {Team}          0.05158730 0.7647059  10.142415
206 {People,Team}                => {Customer}      0.05158730 0.9285714  12.315789
207 {Customer,Team}              => {People}        0.05158730 1.0000000  13.263158
208 {Customer,People}            => {Personnel}     0.05555556 0.8235294  10.922601
209 {People,Personnel}           => {Customer}      0.05555556 1.0000000  13.263158
210 {Customer,Personnel}         => {People}        0.05555556 1.0000000  13.263158
211 {People,Team}                => {Personnel}     0.04761905 0.8571429  11.368421
212 {People,Personnel}           => {Team}          0.04761905 0.8571429  11.368421
213 {Personnel,Team}             => {People}        0.04761905 0.8000000  10.610526
214 {Business,Corporate}         => {Organization}  0.05158730 0.8125000  10.776316
215 {Business,Organization}      => {Corporate}     0.05158730 0.8666667  11.494737
216 {Corporate,Organization}     => {Business}      0.05158730 1.0000000  13.263158
217 {Customer,User}              => {Team}          0.05158730 0.7222222   9.578947
218 {Team,User}                  => {Customer}      0.05158730 1.0000000  13.263158
219 {Customer,Team}              => {User}          0.05158730 1.0000000  13.263158
220 {Customer,User}              => {Personnel}     0.05555556 0.7777778  10.315789
221 {Personnel,User}             => {Customer}      0.05555556 1.0000000  13.263158
222 {Customer,Personnel}         => {User}          0.05555556 1.0000000  13.263158
223 {Team,User}                  => {Personnel}     0.04761905 0.9230769  12.242915
224 {Personnel,User}             => {Team}          0.04761905 0.8571429  11.368421
225 {Personnel,Team}             => {User}          0.04761905 0.8000000  10.610526
226 {Intrusion,Risk}             => {Attack}        0.04761905 1.0000000  13.263158
227 {Attack,Risk}                => {Intrusion}     0.04761905 1.0000000  13.263158
228 {Attack,Intrusion}           => {Risk}          0.04761905 0.6315789   8.376731
229 {Customer,Team}              => {Personnel}     0.04761905 0.9230769  12.242915
230 {Customer,Personnel}         => {Team}          0.04761905 0.8571429  11.368421
231 {Personnel,Team}             => {Customer}      0.04761905 0.8000000  10.610526
232 {Site,Workspace}             => {Space}         0.03968254 0.8333333  11.052632
233 {Space,Workspace}            => {Site}          0.03968254 0.7142857   9.473684
234 {Site,Space}                 => {Workspace}     0.03968254 1.0000000  13.263158
235 {Site,Workspace}             => {Premises}      0.03968254 0.8333333  11.052632
236 {Premises,Workspace}         => {Site}          0.03968254 0.8333333  11.052632
237 {Premises,Site}              => {Workspace}     0.03968254 0.7692308  10.202429
238 {Space,Workspace}            => {Premises}      0.03968254 0.7142857   9.473684
239 {Premises,Workspace}         => {Space}         0.03968254 0.8333333  11.052632
240 {Premises,Space}             => {Workspace}     0.03968254 1.0000000  13.263158
241 {Space,Workspace}            => {Environment}   0.03968254 0.7142857   9.473684
```

```
242 {Environment,Workspace}               => {Space}        0.03968254 0.8333333  11.052632
243 {Environment,Space}                   => {Workspace}    0.03968254 0.8333333  11.052632
244 {Attack,Intrusion}                     => {Event}        0.04365079 0.5789474   7.678670
245 {Event,Intrusion}                      => {Attack}       0.04365079 1.0000000  13.263158
246 {Attack,Event}                         => {Intrusion}    0.04365079 1.0000000  13.263158
247 {Attack,Intrusion}                     => {Incident}     0.05158730 0.6842105   9.074792
248 {Incident,Intrusion}                   => {Attack}       0.05158730 1.0000000  13.263158
249 {Attack,Incident}                      => {Intrusion}    0.05158730 1.0000000  13.263158
250 {Attack,Intrusion}                     => {Target}       0.03968254 0.5263158   6.980609
251 {Intrusion,Target}                     => {Attack}       0.03968254 1.0000000  13.263158
252 {Attack,Target}                        => {Intrusion}    0.03968254 1.0000000  13.263158
253 {Event,Intrusion}                      => {Incident}     0.03968254 0.9090909  12.057416
254 {Incident,Intrusion}                   => {Event}        0.03968254 0.7692308  10.202429
255 {Event,Incident}                       => {Intrusion}    0.03968254 0.6666667   8.842105
256 {Attack,Event}                         => {Incident}     0.03968254 0.9090909  12.057416
257 {Attack,Incident}                      => {Event}        0.03968254 0.7692308  10.202429
258 {Event,Incident}                       => {Attack}       0.03968254 0.6666667   8.842105
259 {Equipment,Server}                     => {Hardware}     0.05555556 1.0000000  13.263158
260 {Equipment,Hardware}                   => {Server}       0.05555556 0.8750000  11.605263
261 {Hardware,Server}                      => {Equipment}    0.05555556 0.8750000  11.605263
262 {Equipment,Server}                     => {Computer}     0.05158730 0.9285714  12.315789
263 {Computer,Equipment}                   => {Server}       0.05158730 0.9285714  12.315789
264 {Computer,Server}                      => {Equipment}    0.05158730 0.8666667  11.494737
265 {Equipment,Network}                    => {Hardware}     0.03968254 1.0000000  13.263158
266 {Equipment,Hardware}                   => {Network}      0.03968254 0.6250000   8.289474
267 {Hardware,Network}                     => {Equipment}    0.03968254 0.8333333  11.052632
268 {Equipment,Hardware}                   => {Computer}     0.05555556 0.8750000  11.605263
269 {Computer,Equipment}                   => {Hardware}     0.05555556 1.0000000  13.263158
270 {Computer,Hardware}                    => {Equipment}    0.05555556 0.8750000  11.605263
271 {Program,Software}                     => {Code}         0.04365079 0.8461538  11.222672
272 {Code,Program}                         => {Software}     0.04365079 0.7857143  10.421053
273 {Code,Software}                        => {Program}      0.04365079 0.8461538  11.222672
274 {Policy,Rule}                          => {Guideline}    0.03968254 0.7692308  10.202429
275 {Guideline,Rule}                       => {Policy}       0.03968254 0.9090909  12.057416
276 {Guideline,Policy}                     => {Rule}         0.03968254 0.7692308  10.202429
277 {Guideline,Plan}                       => {Strategy}     0.03968254 0.9090909  12.057416
278 {Plan,Strategy}                        => {Guideline}    0.03968254 0.6666667   8.842105
279 {Guideline,Strategy}                   => {Plan}         0.03968254 1.0000000  13.263158
280 {Network,Server}                       => {Hardware}     0.04365079 0.9166667  12.157895
281 {Hardware,Server}                      => {Network}      0.04365079 0.6875000   9.118421
282 {Hardware,Network}                     => {Server}       0.04365079 0.9166667  12.157895
283 {Network,Server}                       => {Computer}     0.03968254 0.8333333  11.052632
284 {Computer,Server}                      => {Network}      0.03968254 0.6666667   8.842105
285 {Computer,Network}                     => {Server}       0.03968254 0.9090909  12.057416
286 {Hardware,Server}                      => {Computer}     0.05952381 0.9375000  12.434211
287 {Computer,Server}                      => {Hardware}     0.05952381 1.0000000  13.263158
288 {Computer,Hardware}                    => {Server}       0.05952381 0.9375000  12.434211
289 {Hardware,Network}                     => {Computer}     0.04365079 0.9166667  12.157895
290 {Computer,Network}                     => {Hardware}     0.04365079 1.0000000  13.263158
291 {Computer,Hardware}                    => {Network}      0.04365079 0.6875000   9.118421
292 {People,Stakeholder,User}              => {Customer}     0.05952381 1.0000000  13.263158
293 {Customer,People,Stakeholder}          => {User}         0.05952381 1.0000000  13.263158
294 {Customer,Stakeholder,User}            => {People}       0.05952381 1.0000000  13.263158
295 {Customer,People,User}                 => {Stakeholder}  0.05952381 0.8823529  11.702786
296 {People,Stakeholder,User}              => {Team}         0.04761905 0.8000000  10.610526
297 {People,Stakeholder,Team}              => {User}         0.04761905 1.0000000  13.263158
```

```
298 {Stakeholder,Team,User}              => {People}       0.04761905 1.0000000  13.263158
299 {People,Team,User}                   => {Stakeholder}  0.04761905 0.9230769  12.242915
300 {People,Stakeholder,User}            => {Personnel}    0.05158730 0.8666667  11.494737
301 {People,Personnel,Stakeholder}       => {User}         0.05158730 1.0000000  13.263158
302 {Personnel,Stakeholder,User}         => {People}       0.05158730 1.0000000  13.263158
303 {People,Personnel,User}              => {Stakeholder}  0.05158730 0.9285714  12.315789
304 {Customer,People,Stakeholder}        => {Team}         0.04761905 0.8000000  10.610526
305 {People,Stakeholder,Team}            => {Customer}     0.04761905 1.0000000  13.263158
306 {Customer,Stakeholder,Team}          => {People}       0.04761905 1.0000000  13.263158
307 {Customer,People,Team}               => {Stakeholder}  0.04761905 0.9230769  12.242915
308 {Customer,People,Stakeholder}        => {Personnel}    0.05158730 0.8666667  11.494737
309 {People,Personnel,Stakeholder}       => {Customer}     0.05158730 1.0000000  13.263158
310 {Customer,Personnel,Stakeholder}     => {People}       0.05158730 1.0000000  13.263158
311 {Customer,People,Personnel}          => {Stakeholder}  0.05158730 0.9285714  12.315789
312 {People,Stakeholder,Team}            => {Personnel}    0.04365079 0.9166667  12.157895
313 {People,Personnel,Stakeholder}       => {Team}         0.04365079 0.8461538  11.222672
314 {Personnel,Stakeholder,Team}         => {People}       0.04365079 1.0000000  13.263158
315 {People,Personnel,Team}              => {Stakeholder}  0.04365079 0.9166667  12.157895
316 {Customer,Stakeholder,User}          => {Team}         0.04761905 0.8000000  10.610526
317 {Stakeholder,Team,User}              => {Customer}     0.04761905 1.0000000  13.263158
318 {Customer,Stakeholder,Team}          => {User}         0.04761905 1.0000000  13.263158
319 {Customer,Team,User}                 => {Stakeholder}  0.04761905 0.9230769  12.242915
320 {Customer,Stakeholder,User}          => {Personnel}    0.05158730 0.8666667  11.494737
321 {Personnel,Stakeholder,User}         => {Customer}     0.05158730 1.0000000  13.263158
322 {Customer,Personnel,Stakeholder}     => {User}         0.05158730 1.0000000  13.263158
323 {Customer,Personnel,User}            => {Stakeholder}  0.05158730 0.9285714  12.315789
324 {Stakeholder,Team,User}              => {Personnel}    0.04365079 0.9166667  12.157895
325 {Personnel,Stakeholder,User}         => {Team}         0.04365079 0.8461538  11.222672
326 {Personnel,Stakeholder,Team}         => {User}         0.04365079 1.0000000  13.263158
327 {Personnel,Team,User}                => {Stakeholder}  0.04365079 0.9166667  12.157895
328 {Customer,Stakeholder,Team}          => {Personnel}    0.04365079 0.9166667  12.157895
329 {Customer,Personnel,Stakeholder}     => {Team}         0.04365079 0.8461538  11.222672
330 {Personnel,Stakeholder,Team}         => {Customer}     0.04365079 1.0000000  13.263158
331 {Customer,Personnel,Team}            => {Stakeholder}  0.04365079 0.9166667  12.157895
332 {Intrusion,Risk,Threat}              => {Attack}       0.04761905 1.0000000  13.263158
333 {Attack,Risk,Threat}                 => {Intrusion}    0.04761905 1.0000000  13.263158
334 {Attack,Intrusion,Threat}            => {Risk}         0.04761905 0.8571429  11.368421
335 {Attack,Intrusion,Risk}              => {Threat}       0.04761905 1.0000000  13.263158
336 {Customer,People,User}               => {Team}         0.05158730 0.7647059  10.142415
337 {People,Team,User}                   => {Customer}     0.05158730 1.0000000  13.263158
338 {Customer,People,Team}               => {User}         0.05158730 1.0000000  13.263158
339 {Customer,Team,User}                 => {People}       0.05158730 1.0000000  13.263158
340 {Customer,People,User}               => {Personnel}    0.05555556 0.8235294  10.922601
341 {People,Personnel,User}              => {Customer}     0.05555556 1.0000000  13.263158
342 {Customer,People,Personnel}          => {User}         0.05555556 1.0000000  13.263158
343 {Customer,Personnel,User}            => {People}       0.05555556 1.0000000  13.263158
344 {People,Team,User}                   => {Personnel}    0.04761905 0.9230769  12.242915
345 {People,Personnel,User}              => {Team}         0.04761905 0.8571429  11.368421
346 {People,Personnel,Team}              => {User}         0.04761905 1.0000000  13.263158
347 {Personnel,Team,User}                => {People}       0.04761905 1.0000000  13.263158
348 {Customer,People,Team}               => {Personnel}    0.04761905 0.9230769  12.242915
349 {Customer,People,Personnel}          => {Team}         0.04761905 0.8571429  11.368421
350 {People,Personnel,Team}              => {Customer}     0.04761905 1.0000000  13.263158
351 {Customer,Personnel,Team}            => {People}       0.04761905 1.0000000  13.263158
352 {Customer,Team,User}                 => {Personnel}    0.04761905 0.9230769  12.242915
353 {Customer,Personnel,User}            => {Team}         0.04761905 0.8571429  11.368421
```

```
354 {Personnel,Team,User}                        => {Customer}      0.04761905 1.0000000  13.263158
355 {Customer,Personnel,Team}                    => {User}          0.04761905 1.0000000  13.263158
356 {Attack,Event,Intrusion}                      => {Incident}      0.03968254 0.9090909  12.057416
357 {Attack,Incident,Intrusion}                  => {Event}         0.03968254 0.7692308  10.202429
358 {Event,Incident,Intrusion}                   => {Attack}        0.03968254 1.0000000  13.263158
359 {Attack,Event,Incident}                      => {Intrusion}     0.03968254 1.0000000  13.263158
360 {Equipment,Hardware,Server}                  => {Computer}      0.05158730 0.9285714  12.315789
361 {Computer,Equipment,Server}                  => {Hardware}      0.05158730 1.0000000  13.263158
362 {Computer,Equipment,Hardware}                => {Server}        0.05158730 0.9285714  12.315789
363 {Computer,Hardware,Server}                   => {Equipment}     0.05158730 0.8666667  11.494737
364 {Hardware,Network,Server}                    => {Computer}      0.03968254 0.9090909  12.057416
365 {Computer,Network,Server}                    => {Hardware}      0.03968254 1.0000000  13.263158
366 {Computer,Hardware,Server}                   => {Network}       0.03968254 0.6666667   8.842105
367 {Computer,Hardware,Network}                  => {Server}        0.03968254 0.9090909  12.057416
368 {Customer,People,Stakeholder,User}           => {Team}          0.04761905 0.8000000  10.610526
369 {People,Stakeholder,Team,User}               => {Customer}      0.04761905 1.0000000  13.263158
370 {Customer,People,Stakeholder,Team}           => {User}          0.04761905 1.0000000  13.263158
371 {Customer,Stakeholder,Team,User}             => {People}        0.04761905 1.0000000  13.263158
372 {Customer,People,Team,User}                  => {Stakeholder}   0.04761905 0.9230769  12.242915
373 {Customer,People,Stakeholder,User}           => {Personnel}     0.05158730 0.8666667  11.494737
374 {People,Personnel,Stakeholder,User}          => {Customer}      0.05158730 1.0000000  13.263158
375 {Customer,People,Personnel,Stakeholder}      => {User}          0.05158730 1.0000000  13.263158
376 {Customer,Personnel,Stakeholder,User}        => {People}        0.05158730 1.0000000  13.263158
377 {Customer,People,Personnel,User}             => {Stakeholder}   0.05158730 0.9285714  12.315789
378 {People,Stakeholder,Team,User}               => {Personnel}     0.04365079 0.9166667  12.157895
379 {People,Personnel,Stakeholder,User}          => {Team}          0.04365079 0.8461538  11.222672
380 {People,Personnel,Stakeholder,Team}          => {User}          0.04365079 1.0000000  13.263158
381 {Personnel,Stakeholder,Team,User}            => {People}        0.04365079 1.0000000  13.263158
382 {People,Personnel,Team,User}                 => {Stakeholder}   0.04365079 0.9166667  12.157895
383 {Customer,People,Stakeholder,Team}           => {Personnel}     0.04365079 0.9166667  12.157895
384 {Customer,People,Personnel,Stakeholder}      => {Team}          0.04365079 0.8461538  11.222672
385 {People,Personnel,Stakeholder,Team}          => {Customer}      0.04365079 1.0000000  13.263158
386 {Customer,Personnel,Stakeholder,Team}        => {People}        0.04365079 1.0000000  13.263158
387 {Customer,People,Personnel,Team}             => {Stakeholder}   0.04365079 0.9166667  12.157895
388 {Customer,Stakeholder,Team,User}             => {Personnel}     0.04365079 0.9166667  12.157895
389 {Customer,Personnel,Stakeholder,User}        => {Team}          0.04365079 0.8461538  11.222672
390 {Personnel,Stakeholder,Team,User}            => {Customer}      0.04365079 1.0000000  13.263158
391 {Customer,Personnel,Stakeholder,Team}        => {User}          0.04365079 1.0000000  13.263158
392 {Customer,Personnel,Team,User}               => {Stakeholder}   0.04365079 0.9166667  12.157895
393 {Customer,People,Team,User}                  => {Personnel}     0.04761905 0.9230769  12.242915
394 {Customer,People,Personnel,User}             => {Team}          0.04761905 0.8571429  11.368421
395 {People,Personnel,Team,User}                 => {Customer}      0.04761905 1.0000000  13.263158
396 {Customer,People,Personnel,Team}             => {User}          0.04761905 1.0000000  13.263158
397 {Customer,Personnel,Team,User}               => {People}        0.04761905 1.0000000  13.263158
398 {Customer,People,Stakeholder,Team,User}      => {Personnel}     0.04365079 0.9166667  12.157895
399 {Customer,People,Personnel,Stakeholder,User} => {Team}          0.04365079 0.8461538  11.222672
400 {People,Personnel,Stakeholder,Team,User}     => {Customer}      0.04365079 1.0000000  13.263158
401 {Customer,People,Personnel,Stakeholder,Team} => {User}          0.04365079 1.0000000  13.263158
402 {Customer,Personnel,Stakeholder,Team,User}   => {People}        0.04365079 1.0000000  13.263158
403 {Customer,People,Personnel,Team,User}        => {Stakeholder}   0.04365079 0.9166667  12.157895
```

# APPENDIX E - HIGHER-LEVEL QUESTIONNAIRE

| ID | Question Type 2 High Level | Subtype | Covers |
|---|---|---|---|
| 1 | Given the definition of digital forensic readiness (DFR) as the state of preparedness to obtain, understand, and present verifiable digital evidence when needed, I would rate my organization's DFR as: | Perceived | 40 |
| 2 | Management is convinced of the importance of digital forensic readiness | Perceived | 8 |
| 3 | Implementing a digital forensics program is expensive. | Perceived | 9 |
| 4 | This organization is exposed to many risks and threats. | Perceived | 10 |
| 5 | Our firm has a public profile. | Demographic | 11 |
| 6 | The location(s) of the organization makes it insecure. | Perceived | 12, 16 |
| 7 | The organization's policies on information systems monitoring are consistent with its personnel privacy policies and applicable employment law. | Perceived | 29, 178 |
| 8 | The organization's personnel is committed to the forensics program and implement lessons learned from previous incidents. | Perceived | 32, 36 |
| 9 | The organization's employees have knowledge of information management and security policies. | Perceived | 34, 37, 143 |
| 10 | The organization's security system has been proven to be reliable. | Perceived | 39, 102, 136, 186, 145 |
| 11 | Information technology and information security objectives are aligned with the business mission and objectives. | Perceived | 177 |
| 12 | Fulfilling the demands that the legal system makes about admissibility and reliability of digital evidence for our organization is: | Perceived | 179 |
| 13 | Seeks accountability for intruders. | Does | 7, 43 |
| 14 | Allows wireless access. | Does | 20 |
| 15 | Enforces forensic policies and makes staff accountable of their digital forensic responsibilities and the use of digital forensic tools. | Does | 27, 123, 187 |
| 16 | Offers and encourages personnel training and guidance in secure conduct and digital forensics tools and techniques. | Does | 13, 31, 33, 38, 123, 157, 166 |
| 17 | Uses digital forensics tools and techniques, e.g., intrusion detection systems (IDS), security event management software (SEM), forensic kits, antivirus and spyware. | Does | 43, 100, 101, 145, 152, 181, 184 |
| 18 | Identifies and prioritizes the sources of evidence, preserves logs and data, and assesses the value of potential evidence. | Does | 61, 76, 80, 85, 86, 87, 99, 106, 121,155, 188 |
| 19 | Controls information flow and channels to prevent anonymous activities and anti-forensic activities (e.g. password crackers, key-loggers, and steganography software) and assesses Internet activities such as cookies, temporary files, URLs, email, instant messages and SMTP send-receiver pairs. | Does | 88, 92, 145, 159 |
| 20 | Develops the digital and physical infrastructure with forensic capabilities such as authentication traffic monitoring, tamper proof mechanisms and logging time synchronization. | Does | 89, 100, 159, 182, 185 |

|  |  |  |  |
|---|---|---|---|
| 21 | Controls access to data and evidence through strong authentication, access control lists, user logging, encryption, and implements measures for handling inadvertent exposures. | Does | 81, 91, 93, 96, 97, 98, 103, 145 |
| 22 | Bans disk scrubbing tools, file shredding software, personal file encryption, and anti-forensic strategies (e.g. anonymity, data destruction/alteration, and onion routing). | Does | 104, 152 |
| 23 | Looks for legal and technical advice, including published standards, regarding forensic policies, procedures, and information security, and monitors emerging academic digital forensics research. | Does | 111, 167, 168, 170, 172, 174 |
| 24 | Conducts regular risk assessments and compliance reviews. | Does | 112, 156, 173 |
| 25 | Profiles and monitors systems' users and their personal devices. | Does | 137, 138, 139, 140 |
| 26 | Controls physical access to, classifies, and relocates corporate physical and digital assets according to a digital forensic program. | Does | 47, 57, 147, 151 |
| 27 | Develop corporate policies and procedures collaboratively using collaboration tools to maintain a shared workspace. | Does | 160 |
| 28 | Controls security information through dashboards and metrics that continuously and dynamically measure information security performance. | Does | 169 |
| 29 | Manages external digital forensic investigators, establishes their capabilities and response times, and validates the accreditation of their laboratories. | Does | 171 |
| 30 | Performs security benchmarking to assess the preparedness of competitors and enemies. | Does | 175 |
| 31 | A forensic culture of preserving evidence and sharing knowledge in computer security and digital forensics. | Has | 5 |
| 32 | A corporate culture of secrecy (forensics activities are kept from users). | Has | 6 |
| 33 | Policies clarifying ownership of data in corporate and personnel devices, use of systems, privacy, and consent of monitoring. | Has | 22, 23, 26 |
| 34 | Policies defining potential incidents and how to respond to them. | Has | 14, 21, 24, 25, 26, 74, 75, 105, 113, 116 |
| 35 | Policies clarifying the roles and tasks to comply with statutory and/or governmental regulations (e.g. Sarbanes–Oxley, HIPAA, admissibility rules, reporting requirements, international law and penalties for security incidents). | Has | 28, 77, 107, 109, 116, 125, 180 |
| 36 | A documented digital forensics investigation protocol describing roles and procedures to capture, store, map, analyze, preserve, control access to, integrate, and present evidence. | Has | 30, 26, 48, 74, 78, 110, 114, 115, 120 121, 127, 128, 129, 130, 131 |
| 37 | A quality assurance system, with good records, that covers policies, activities, procedures, training, roles, documentation, and management. | Has | 41, 56 |
| 38 | A documented system security architecture configuration with consistent standards throughout the entire platform. | Has | 46, 54, 90 |

| | | | |
|---|---|---|---|
| 39 | Archived reports of previous incidents, anomalous observations, crime and dispute history and lessons learned. | Has | 49, 50, 51 |
| 40 | A change management database that includes file hashes for common operating system files and for deployed applications, using file integrity checking software on important assets. | Has | 52, 53 |
| 41 | A proper laboratory, equipment, hardware and software for onsite computer forensic examiners. | Has | 58, 59, 189 |
| 42 | A secure storage of systems and networks activity logs with the associated meta-data identifying times and authors. | Has | 55, 84, 94, 95 |
| 43 | A suspicion policy to review potential sources of attacks or failure, complaints, crimes and disputes, and threats from opportunists, competitors or disgruntled employees. This policy indicates how to manage people leaving the company. | Has | 108 |
| 44 | Archive management procedures to assure that records (including those in the cloud) possess content, context and structure, while preserving evidence quality in terms of authenticity, reliability, integrity, and usability. | Has | 115 |
| 45 | Procedures describing the configuration and use of active monitoring and logging mechanisms, including procedures to prevent alteration of intercepted communications. | Has | 117 |
| 46 | Information security audit procedures that include protection of IT and business systems, and monitoring of the forensics process. | Has | 118, 119 |
| 47 | Procedures for performing backups, gathering permanent and volatile data, and analyzing admissible evidence. | Has | 120, 122, 124, 163 |
| 48 | A process for the selection, use, testing, and maintenance of technology deployed in the organization's information systems and the forensic readiness program. | Has | 126, 149 |
| 49 | The technology, expertise, and resources to perform computer and network forensics and manage legal evidence properly. | Has | 35, 132, 141, 144, 146, 148, 150, 153 |
| 50 | Dedicated roles relating to security and forensics including first responders and investigators ready to work collaboratively with legal, IT, law enforcement, business, and auditing representatives in case of a cyber incident. | Has | 133, 134, 135, 142, 161, 162, 176 |
| 51 | Sufficient decryption capabilities to counter the increasingly pervasive use of encryption technologies. | Has | 154 |
| 52 | A business continuity plan to minimize interruption to the business while gathering admissible evidence, to restore essential services during an attack, to avoid financial loss, and to recover assets and data. | Has | 158 |
| 53 | Mature and adequate governance models as well as an information systems development life cycle (ISDLC) informed by a well-developed forensic readiness policy. | Has | 45, 46, 164, 165 |
| 54 | Storage technology that is appropriate in capacity and functionality, including storage visualization abilities. | Has | 190 |
| 55 | Multiple virtual locations, wired and wireless networks, and/or a mobile platform. | Demographic | 60 |
| 56 | Enough funding for the implementation of digital forensic readiness. | Demographic | 42 |
| 57 | The standards of the digital forensics discipline and how to conduct an onsite examination keeping the integrity of the original evidence. | Knows | 15, 19, 125, 174 |

| | | | |
|---|---|---|---|
| 58 | Whether or not to turn off a hacked system or device in case of a cyber incident. | Knows | 17 |
| 59 | How to handle a politically sensitive or publicly embarrassing incident. | Knows | 11, 18 |
| 60 | Which forensic tools and techniques the organization needs to deploy in case of a cyber incident. | Knows | 63, 123 |
| 61 | Where to look in the system to identify case specific evidence in case of a cyber incident. | Knows | 64 |
| 62 | How to anticipate the organization's discovery needs and accelerate its investigation in case of a cyber incident. | Knows | 65 |
| 63 | How to forecast and control the escalation of costs when facing a digital forensic incident. | Knows | 66 |
| 64 | How to determine whether a warrant allows for an onsite or in situ examination, seizure and removal of the system(s), in case of a cyber incident. | Knows | 67 |
| 65 | How to recognize the range of personnel within the firm who may be involved in a legal inquiry, in case of a cyber incident. | Knows | 62, 68 |
| 66 | How to determine the location, remote access methods, time, timeline of events, and duration of a cyber incident. | Knows | 69, 70 |
| 67 | How to determine the nature, crime category, types of technologies used or involved, and technical skill and knowledge of a suspect in a cyber incident. | Knows | 62, 71, 72, 73 |
| 68 | How to provide detailed log and documentation of the chain of evidence at every step, including information about the tools used, in case of a cyber incident. | Knows | 79 |
| 69 | The sources and format of the organization's  data, when and where data is generated, the associated threats to the data, and how data is preserved for long-term storage. | Knows | 83 |
| 70 | How to demonstrate due diligence and compliance with the organization’'s policies and all applicable laws and regulations in all phases of a forensic investigation process. | Knows | 125 |
| 71 | Industry sector of the organization. | Demographic | 1 |
| 72 | What are the estimated organization sales? (in thousands of dollars per year). | Demographic | 2 |
| 73 | What is the organization size in number of employees? | Demographic | 3 |
| 74 | What is the organization size in number of customers? | Demographic | 4 |
| 75 | What is the amount of data produced in the organization every month? | Demographic | 82 |
| 76 | After completing this survey and given the definition of digital forensic readiness (DFR) as the state of preparedness to obtain, understand, and present verifiable digital evidence when needed, I would rate my organization's DFR as: | Perceived | 191 |

## APPENDIX F – FINAL SURVEY

Thanks for your participation in this study. By agreeing to participate in this survey you consent with the utilization of this information for the purpose of the study and acknowledge that your participation is voluntary. You can abandon this this survey at any time. However, we appreciate that you complete all required information to the best of your knowledge.

Choices: Accept, Decline

Please read each sentence carefully and check the circle corresponding to your level of agreement with it according to your perception of the situation in your organization.

1. Given the definition of digital forensic readiness (DFR) as the state of preparedness to obtain, understand, and present verifiable digital evidence when needed, I would rate my organization's DFR as:

Choices: Very low, Low, Average, High, Very high

Question Matrix:
2. Management is convinced of the importance of digital forensic readiness
3. Implementing a digital forensics program is expensive.
4. This organization is exposed to many risks and threats.
5. Our firm has a public profile.
6. The location(s) of the organization makes it insecure.
7. The organization's policies on information systems monitoring are consistent with its personnel privacy policies and applicable employment law.
8. The organization's personnel is committed to the forensics program and implement lessons learned from previous incidents.
9. The organization's employees have knowledge of information management and security policies.
10.The organization's security system has been proven to be reliable.
11.Information technology and information security objectives are aligned with the business mission and objectives.
12.Fulfilling the demands that the legal system makes about admissibility and reliability of digital evidence for our organization is hard.

Choices: Strongly agree, Agree, Neither agree nor disagree, Disagree, Strongly disagree

Question Matrix:
Please select your level of agreement with the following assertions of what your organization currently does.

13.Seeks accountability for intruders.
14.Allows wireless access.
15.Enforces forensic policies and makes staff accountable of their digital forensic responsibilities and the use of digital forensic tools.
16.Offers and encourages personnel training and guidance in secure conduct and digital forensics tools and techniques.
17.Uses digital forensics tools and techniques, e.g., intrusion detection systems (IDS), security event management software (SEM), forensic kits, antivirus and spyware.
18.Identifies and prioritizes the sources of evidence, preserves logs and data, and assesses the value of potential evidence.
19.Controls information flow and channels to prevent anonymous activities and anti-forensic activities (e.g. password crackers, key-loggers, and steganography software) and assesses Internet activities such as cookies, temporary files, URLs, email, instant messages and SMTP send-receiver pairs.
20.Develops the digital and physical infrastructure with forensic capabilities such as authentication traffic monitoring, tamper proof mechanisms and logging time synchronization.
21.Controls access to data and evidence through strong authentication, access control lists, user logging, encryption, and implements measures for handling inadvertent exposures.

22.Bans disk scrubbing tools, file shredding software, personal file encryption, and anti-forensic strategies (e.g. anonymity, data destruction/alteration, and onion routing).
23.Looks for legal and technical advice, including published standards, regarding forensic policies, procedures, and information security, and monitors emerging academic digital forensics research.
24.Conducts regular risk assessments and compliance reviews.
25.Profiles and monitors systems' users and their personal devices.
26.Controls physical access to, classifies, and relocates corporate physical and digital assets according to a digital forensic program.
27.Develops corporate policies and procedures collaboratively using collaboration tools to maintain a shared workspace.
28.Controls security information through dashboards and metrics that continuously and dynamically measure information security performance.
29.Manages external digital forensic investigators, establishes their capabilities and response times, and validates the accreditation of their laboratories.
30.Performs security benchmarking to assess the preparedness of competitors and enemies.

Choices: Strongly agree, Agree, Neither agree nor disagree, Disagree, Strongly disagree

Question Matrix:
Please select your level of agreement with the following assertions of what your organization currently has.

31.A forensic culture of preserving evidence and sharing knowledge in computer security and digital forensics.
32.A corporate culture of secrecy (forensics activities are kept from users).
33.Policies clarifying ownership of data in corporate and personnel devices, use of systems, privacy, and consent of monitoring.
34.Policies defining potential incidents and how to respond to them.
35.Policies clarifying the roles and tasks to comply with statutory and/or governmental regulations (e.g. Sarbanes–Oxley, HIPAA, admissibility rules, reporting requirements, international law, and penalties for security incidents).
36.A documented digital forensics investigation protocol describing roles and procedures to capture, store, map, analyze, preserve, control access to, integrate, and present evidence.
37.A quality assurance system, with good records, that covers policies, activities, procedures, training, roles, documentation, and management.
38.A documented system security architecture configuration with consistent standards throughout the entire platform.
39.Archived reports of previous incidents, anomalous observations, crime and dispute history and lessons learned.
40.A change management database that includes file hashes for common operating system files and for deployed applications, using file integrity checking software on important assets.
41.A proper laboratory, equipment, hardware and software for onsite computer forensic examiners.
42.A secure storage of systems and networks activity logs with the associated meta-data identifying times and authors.
43.A suspicion policy to review potential sources of attacks or failure, complaints, crimes and disputes, and threats from opportunists, competitors or disgruntled employees. This policy indicates how to manage people leaving the company.
44.Archive management procedures to assure that records (including those in the cloud) possess content, context and structure, while preserving evidence quality in terms of authenticity, reliability, integrity, and usability.
45.Procedures describing the configuration and use of active monitoring and logging mechanisms, including procedures to prevent alteration of intercepted communications.
46.Information security audit procedures that include protection of IT and business systems, and monitoring of the forensics process.
47.Procedures for performing backups, gathering permanent and volatile data, and analyzing admissible evidence.

48.A process for the selection, use, testing, and maintenance of technology deployed in the organization's information systems and the forensic readiness program.
49.The technology, expertise, and resources to perform computer and network forensics and manage legal evidence properly.
50.Dedicated roles relating to security and forensics including first responders and investigators ready to work collaboratively with legal, IT, law enforcement, business, and auditing representatives in case of a cyber incident.
51.Sufficient decryption capabilities to counter the increasingly pervasive use of encryption technologies.
52.A business continuity plan to minimize interruption to the business while gathering admissible evidence, to restore essential services during an attack, to avoid financial loss, and to recover assets and data.
53.Mature and adequate governance models as well as an information systems development life cycle (ISDLC) informed by a well-developed forensic readiness policy.
54.Storage technology that is appropriate in capacity and functionality, including storage visualization abilities.
55.Multiple virtual locations, wired and wireless networks, and/or a mobile platform.
56.Enough funding for the implementation of digital forensic readiness.

Choices: Strongly agree, Agree, Neither agree nor disagree, Disagree, Strongly disagree

Question Matrix:
Please select your level of agreement with whether or not the people in your organization in charge of the following tasks has the knowledge to perform them.

57.How to conduct an onsite examination keeping the integrity of the original evidence.
58.Whether or not to turn off a hacked system or device in case of a cyber incident.
59.How to handle a politically sensitive or publicly embarrassing incident.
60.Which forensic tools and techniques the organization needs to deploy in case of a cyber incident.
61.Where to look in the system to identify case specific evidence in case of a cyber incident.
62.How to anticipate the organization's discovery needs and accelerate its investigation in case of a cyber incident.
63.How to forecast and control the escalation of costs when facing a digital forensic incident.
64.How to determine whether a warrant allows for an onsite or in situ examination, seizure and removal of the system(s), in case of a cyber incident.
65.How to recognize the range of personnel within the firm who may be involved in a legal inquiry, in case of a cyber incident.
66.How to determine the location, remote access methods, time, timeline of events, and duration of a cyber incident.
67.How to determine the nature, crime category, types of technologies used or involved, and technical skill and knowledge of a suspect in a cyber incident.
68.How to provide detailed log and documentation of the chain of evidence at every step, including information about the tools used, in case of a cyber incident.
69.What the sources and format of the organization's data are, when and where data is generated, the associated threats to the data, and how data is preserved for long-term storage.
70.How to demonstrate due diligence and compliance with the organization's policies and all applicable laws and regulations in all phases of a forensic investigation process.

Choices: Strongly agree, Agree, Neither agree nor disagree, Disagree, Strongly disagree

Organizational demographics

1. What is your organization's primary business activity? (Select one only)

Choices:

Manufacturing and Process Industries (Non-computer)

Online Retailer
Internet Service Provider (ISP) or Application Service Provider (ASP)
Communications Carrier
Aerospace
Banking/Finance/Accounting
Insurance/Real Estate/Legal
Federal Government (including military)
State/Local Government
Medical/Dental/Healthcare
Transportation/Utilities
Construction/Architecture/Engineering
Data Processing Services
Wholesale/Retail/Distribution
Education
Marketing/Advertising/Entertainment
Research/Development Lab
Business Services/Consultant
Computer Manufacturer (Hardware, software, peripherals)
Computer/Network Services/Consultant
Computer Related Retailer/Wholesaler/Distributor
Other

2. What are the estimated organization sales? (in thousands of dollars per year).

Choices:

Less than 50
Between 50 and 200
Between 200 and 500
Between 500 and 2,000
More than 2,000

3. What is the organization size in number of employees?

Choices:

1 to 50
Between 51 and 200
Between 201 and 500
Between 501 and 2000
More than 5,000

4. What is the organization size in number of customers?

Choices:

1 to 20
Between 21 and 200
Between 201 and 1,000
Between 1,001 and 10,000
More than 10,000

5. What is the amount of data produced in the organization every month?

Choices:

Less than 10 MB
Between 10 and 500 MB
Between 0.5 and 50 GB
Between 50 GB and 1 TB
More than 1 TB

6. After completing this survey and given the definition of digital forensic readiness (DFR) as the state of preparedness to obtain, understand, and present verifiable digital evidence when needed, I would rate my organization's DFR as:

Choices: Very low, Low, Average, High, Very high

Basic demographics questions:

1. What is your age range in years?

Choices:

Below 18
18 to 25
26 to 40
41 to 60
Above 60

2. What is your gender?

Choices:

Male
Female
Omit to answer

3. For how many years have you been in this organization?

Choices:

Less than 2
2 to 5
6 to 10
11 to 20
More than 20

4. What is your current position in this organization?

5. For how many years have you been in your current position?

Choices:

Less than 2
2 to 5
6 to 10
11 to 20
More than 20

6. Let us know if you have any comments about this survey and add your email if you want to be contacted.

# VITA

## ANDRÉS F. DÍAZ LÓPEZ

### Education

Interdisciplinary Certificate in Applied Statistics
University, Mississippi - May 2016
*University of Mississippi*

MBA Emphasis in Computer Information Systems
Canyon, Texas - Dec. 16, 2011
*West Texas A&M University*

Graduate Specialization in Marketing
Bogotá, Colombia - Dec. 25, 2008
*EOI Madrid School of Business*

Bachelor of Science - Industrial Engineering
Cali, Colombia - May 8, 1998
*Pontificia Universidad Javeriana Cali*

### Academic Experience

Graduate Assistant - *University of Mississippi*
University, Mississippi. Aug. 2012 - Aug. 2017

Instructor of Information Systems - *University of Mississippi*
University, Mississippi. Aug. 2013 - May 2015

Graduate Assistant - *West Texas A&M University*
Canyon, Texas. Jan. 2010 - Dec. 2011

Instructor of Information Systems - *Universidad Javeriana Bogotá*
Bogotá, Colombia, June 2008 - Dec. 2008

Instructor of Technology Management - *Universidad Konrad Lorenz*
Bogotá, Colombia, Jan. 2006 - Dec. 2006

Instructor of Information Systems - Universidad Politécnico Grancolombiano
Bogotá, Colombia, June 2004 - May 2005

Instructor in the Cultural and Sports Department - *Universidad Javeriana Cali*
Cali, Colombia, 1995

**Research Activity**

Díaz López, A. & Reithel, B. J. (2017). A Multidimensional Framework for Digital Forensic Readiness. *Submitted to an ACM journal*.

Díaz López, A. (2015). Proposal for an introductory class of a multi-disciplinary program in digital forensics. *Proceedings of the 2015 Information Systems Education Conference*.

Díaz López, A. (2015). Assessing the ability to act without moving - the movirtuality index. *Proceedings of the 21st Americas Conference on Information Systems.*

Díaz López, A., Guo, X., & Pumphrey, D. (2013). Multidimensional charts. *Proceedings of the 19th Americas Conference on Information Systems.*

Guo, X. & Díaz López, A. (2013). Mobile decision support system usage in organizations. *Proceedings of the 19th Americas Conference on Information Systems.*

Furner, C., Racherla, P., & Zhu, Z. (2012). Uncertainty, trust and purchase intention based on online product reviews: an introduction to a multinational study. *International Journal of Networking and Virtual Organisations 10*, *11*(3-4), 260-276.
(Acknowledgement for data collection and translation of surveys into Spanish)

Diaz López, A., Mengesha, E. & Brown, T. (2010). Impact of the Smart Classrooms in recruitment and academic success in West Texas A&M University. *Poster session presented at the 8th Annual Pathways Student Research Symposium of the Texas A&M University system, Canyon, Texas.*
(First place for a poster in the category of Business and Computer Information Systems)

Díaz López, A. (2010). Impact of the Smart Classrooms in recruitment and academic success in West Texas A&M University: A Data Mining Analysis. *Proceedings of the 17th Student Research Conference of the West Texas A&M University, Canyon, Texas.*
(First place for oral presentation in the category of Business)

**Other Work Experience**

Consultant - *E-Nova*
Bogotá, Colombia. June 2007 to Apr. 2009
Created and managed the company; developed the marketing material and web page; provided consulting for the implementation of Moodle virtual education platforms.

Marketing & Sales Engineer - *Symtek S.A. (Thermo Agent)*
Bogotá, Colombia. Sep. 2002 to May 2007
Performed marketing research; managed projects for international corporate clients; structured and developed managing tools, marketing material, and web design; organized seminars and other events; led marketing area activities for the quality certification ISO 9001 v. 2000.

Project Manager - *Moloko S.A.*
Bogotá, Colombia. June 2000 to June 2002
Led a team of developers of internet sites, intranets, and multimedia projects for organizations, including Fortune 500 companies and the Colombian Government; created processes and tools for the management and measurement of projects.

Sales Representative - *Fesa S.A. (Carvajal Group)*
Cali, Colombia. June 1998 to Feb. 2000

Sold formats, hardware, and software for information handling; provided consulting in information handling and cost savings for customers.
Professional Service

Senator of the Graduate Student Council of the University of Mississippi, 2015 - 2017
Ad hoc reviewer of papers and volunteer for AMCIS, 2016
Volunteer for ICIS, 2015
Session chair and collaborator for ISECON, 2015
Ad hoc reviewer of papers and volunteer for AMCIS, 2015
Ad hoc reviewer of papers for AMCIS, 2013
University ambassador during AACSB final accreditation visit to West Texas A&M University, 2012

**Recognitions**

University of Mississippi representative for SEC Symposium Creativity, Innovation, and Entrepreneurship, Sep. 2015, Atlanta, GA
Doctoral consortium, 2015, AMCIS, Puerto Rico
Patent pending holder of an utility patent in the USPTO, 2014 Alexandria, VA
Finalist, Aug. 2011, The Human Potential Index Challenge of Innocentive and The Economist
Good Neighbor Scholarship, 2011-2012, The State of Texas
College of Business Scholarship, 2011-2012, West Texas A&M University
First place in the 17th Annual Student Research Conference, Business & Computers Systems category, 2011, West Texas A&M University
First place in the 8th Annual Pathways Student Research Symposium, Business & Computers Systems category, 2010, Texas A&M University System
Highest GPA in the Marketing Specialization, 2008, EOI Madrid School of Business, Bogotá

**Competencies**

Spanish: fluent. English: fluent. French: intermediate.
Experience with statistical tools: SPSS, G-Power, SAS, and R.
Experience with programming languages: Python, Visual Basic, PHP, C#.
Experience with data management tools: R Studio, Access, Excel with Data Mining Add-ins and VBA, MySQL, Oracle SQL Developer, PL-SQL and Arc GIS.
Experience with management tools: MS Visio, MS Project, IBM Rational, Qualtrics, Moodle and Blackboard.
Experience with multimedia tools: Prezi, Wix, PowerPoint, HTML, Visual Studio, Audacity, Sonar, Dreamweaver, Illustrator and Flash.