A Framework for Assessing the Core Capabilities of a Digital Forensic Organization

Ahmed Almarzooqi, Andrew Jones

Chapter 3

A FRAMEWORK FOR ASSESSING THE CORE CAPABILITIES OF A DIGITAL FORENSIC ORGANIZATION

Ahmed Almarzooqi and Andrew Jones

Abstract This chapter describes a framework for building and managing the capabilities of digital forensic organizations. The framework employs equations that express the relationships between core capabilities, enabling the definition of digital forensic capabilities. Straussian grounded theory is used to create the theoretical framework that is grounded in the data. The framework is also grounded in the literature on digital forensic capabilities, specifically research related to digital forensic readiness, capability maturity models, digital forensic management frameworks and best practices for building and managing digital forensic laboratories. Thus, the framework is readily integrated with other theories; indeed, it can identify gaps existing in the theories and provides opportunities to extend the theories.

Keywords: Digital forensic readiness, grounded theory, capability maturity model

1. Introduction

Research in digital forensics primarily focuses on the quality of evidence, enhancing the investigation process and developing tools [3, 14]. However, limited research has focused on the decisions made when building and managing the capabilities of a digital forensic organization. To begin with, digital forensics lacks a definition of what constitutes the "capabilities" of a digital forensic organization.

This research surveyed more than thirty digital forensic experts from the United Kingdom and United Arab Emirates on building and managing the capabilities of a digital forensic organization. The participants discussed two types of capabilities. One type of capability covers the ability of an organization to perform digital forensic investigations. An-

other is an organization's capabilities as a whole, where digital forensic investigations are only part of the capabilities. For both types of capabilities, the survey participants were almost unanimous in stating the lack of, and the need for, guidance on specifying capabilities and standards for building and managing the capabilities of digital forensic organizations. While there have been numerous proposals on creating standards, models and frameworks for the digital investigation process [19], no unified standard or framework exists for developing, managing and implementing digital forensic capabilities in organizations, whether in the public (law enforcement) or private (corporate) domains.

This chapter proposes the Digital Forensic Organization Core Capability (DFOCC) Framework as a tool for understanding, improving and standardizing the creation and management of the capabilities of digital forensic organizations. The framework provides a roadmap for developing the capabilities of digital forensic organizations, identifying success factors and creating an attainable universal benchmark that could be used in place of timely and costly accreditation processes.

2. Research Methodology

The proposed framework employs grounded theory [8], a method for discovering theories based on an analysis of the data and explaining participant behavior. Grounded theory focuses on actions and interactions. Since the research attempted to identify patterns in the actions and interactions involved in the development and management of the capabilities of a digital forensic organization, the questions of how and why digital forensic organizations and individual stakeholders understand and develop digital forensic capabilities are best suited to the application of grounded theory.

Martin and Turner [13] define a grounded theory methodology as "an inductive theory discovery methodology that allows the researcher to develop a theoretical account of the general features of a topic while simultaneously grounding the account in empirical observations or data." In short, the goal of grounded theory is to propose a theory. This research attempts to use the proposed DFOCC framework, which was discovered from the data and systematically obtained from social science research, to explore the integral social relationships and the behavior of groups in a digital forensic organization. The primary goal is to understand and explain the development and management of the capabilities of digital forensic organizations.

The core categories of the proposed framework emerged from the data through the three stages of coding processes in Straussian grounded the-

ory, namely, open, axial and selective coding [4, 15]. After a review of the data using the grounded theory coding processes and after examining the relationships between the core categories at the dimensional level, four core categories emerged from the categories and subcategories: (i) policy; (ii) people; (iii) infrastructure; and (iv) investigation. By applying grounded theory, it was possible to understand the relationships between abstract concepts in digital forensic organizations that were derived from categories and grouped as core categories at abstract levels. Although a theory is automatically grounded when using a grounded theory method, it was possible to demonstrate specific instances where the theory connects to concepts and phenomena in the data and to validate the data during the axial and selective coding phases as required by grounded theory. Validation was performed through subsequent interviews and by examining the fit, relevance, workability and modifiability of the theory.

3. Related Work

A review of the literature was performed before conducting the participant interviews. This review also served as a form of validation in grounded theory. Straussian grounded theory allows researchers to consult the literature before starting data collection and data analysis [4]. Four areas of digital forensics research validated the focus on and the need to create a framework for building and managing the capabilities of digital forensic organizations: (i) digital forensic readiness [16]; (ii) capability maturity models [1, 12]; (iii) digital forensic management frameworks [9]; and (iv) best practices for building and managing digital forensic laboratories [11].

3.1 Digital Forensic Readiness

The research of Grobler [9] validates the need for creating a framework for building and managing the capabilities of digital forensic organizations. In particular, Grobler discusses the implementation of digital forensic capabilities in the context of digital forensic readiness, one of the principal challenges in digital forensics. According to Rowlingson [16], digital forensic readiness is "the ability of an organization to maximize its potential to use digital evidence when required." Digital forensic readiness, therefore, does not address the capabilities of a digital forensic organization that conducts investigations, but rather a non-digital-forensic organization that receives the services and/or products of a digital forensic organization. In this regard, digital forensic readiness is not only insufficient, but also not relevant to the capabilities

of a digital forensic organization. Digital forensic readiness prepares the clients of digital forensic organizations whereas the proposed DFOCC framework prepares the digital forensic organizations themselves.

Regardless, digital forensic readiness is a key component of the digital forensic investigation process because its implementation assists digital forensic investigators even before incidents or crimes have occurred. Therefore, digital forensic readiness is proactive rather than reactive in nature. Von Solms et al. [20] have proposed a digital control framework that takes into account digital forensic readiness to provide governance for the digital forensic investigation process. However, this digital forensic control framework does not address the development and management of the capabilities of digital forensic organizations.

3.2 Capability Maturity Model

The literature survey also reviewed efforts focused on applying the capability maturity model to building and managing the capabilities of a digital forensic organization [1, 9, 12]. The capability maturity model has been applied in two contexts: (i) digital forensic investigation context; and (ii) digital forensic capability context. Before explaining the limits of the capability maturity model with regard to explaining digital forensic organization capabilities, it is important to first explain the capability maturity model and its origins. Next, the application of the capability maturity model in digital forensic investigations is discussed. This is followed by the application of the capability maturity model to digital forensic capabilities. Finally, it is shown that the capability maturity model can complement a digital forensic capability framework, but it does not, by itself, achieve a comprehensive view of digital forensic capabilities.

The capability maturity model is used to "describe the degree to which an organization applies formali[z]ed processes to the management of its various business functions" [12]. The model usually applies five levels of maturity in determining the capability levels of an organization's processes. The model was first used in software engineering as an objective assessment tool to measure the abilities of government contractor processes to perform software projects. The capability maturity model was later applied to other disciplines and process areas as a framework for process improvement.

Kerrigan [12] applied the capability maturity model to digital forensic investigations after reviewing several digital forensic investigation frameworks and models. Kerrigan specifically noted that the capability maturity model had to be applied keeping in mind three important and

interrelated concepts: (i) people; (ii) process; and (iii) technology. Kerrigan identified five levels of maturity: (i) ad hoc; (ii) performed; (iii) defined; (iv) managed; and (v) optimized. The five levels were applied to the three key factors (people, process and technology) of organizational capabilities to conduct digital forensic investigations. Of the three key factors, only process was broken down to lower types of actions and interactions.

While Kerrigan [12] extended the capability maturity model to digital forensic investigations, the model was not applied to building and managing digital forensic organization capabilities. In other words, Kerrigan's focus was on the investigative process. An advantage of Kerrigan's approach is that it recognizes the role of people and technology in the digital forensic investigation process. However, the approach fails to express specific actions/interactions in the people and technology categories that would clarify the relationships between the categories.

Al-Hanaei and Rashid [1] have applied the capability maturity model to the capabilities of a digital forensic organization. Their model has six levels of maturity that are largely similar to Kerrigan's five levels. Additionally, like Kerrigan's model, the model considers improvements to the process, tools (technology) and skills (people). Unfortunately, like Kerrigan's model, the model of Al-Hanaei and Rashid does not address the development and management of the capabilities of digital forensic organizations. Also, it fails to clarify how the tools and technology are to be improved.

One reason for the silence of capability maturity models on the detailed relationships and requirements of people and technology is their inherent limitation in explaining the capabilities of a digital forensic organization. A capability maturity model focuses mainly on the process because, by definition, the model is a tool for improving or enhancing existing business processes. Furthermore, unlike the proposed DFOCC framework, a capability maturity model fails to take policy into full consideration as a core capability. Finally, because a capability maturity model is concerned more with improving existing processes within an organization, it is not helpful with regard to building or developing the capabilities of an organization or determining standard minimum requirements for the capabilities.

Nevertheless, the capability maturity model could enhance the proposed DFOCC framework, where DFOCC serves as the roadmap for a digital forensic organization to create a benchmark. While the capability maturity model literature suggests that the model can be used to set benchmarks, its application to a digital forensic organization is difficult because the model does not consider the detailed actions and

Table 1. Comparison of DFMF dimensions and DFOCC categories.

DFMF	DFOCC
Legal and Judicial	N/A
Governance	N/A
Policy	Policy
Process	Investigation
People	People
Technology	Infrastructure

interactions and the relationships between the capabilities. A capability maturity model, for example, would not suggest that there must be at least two types of tools and two investigators as a benchmark. This is because the model determines a benchmark based on the clients' existing capabilities, whether or not the perceived capabilities meet the definition of capabilities under the proposed DFOCC framework.

3.3 Digital Forensics Management Framework

The Digital Forensic Management Framework (DFMF) of Grobler [9] is most relevant to building and managing digital forensic organization capabilities. Grobler categorized individual actions in a comprehensive investigation model to identify the dimensions of digital forensics. He then constructed the framework based on these dimensions, which, interestingly, match the core categories of the DFOCC framework that is based on grounded theory.

Table 1 compares the DFMF dimensions with the DFOCC categories. The table clearly reveals the similarities and differences between DFMF and DFOCC. The basic similarities are the four common core capabilities of a digital forensic organization: (i) policy; (ii) process/investigation; (iii) people; and (iv) technology/infrastructure. DFMF adds legal and judicial and governance as additional dimensions whereas DFOCC identifies these two concepts using a conditional matrix as affecting capabilities, albeit not as core capabilities. It appears that the only differences are the wording – DFMF uses process and technology while DFOCC uses investigation and infrastructure, respectively.

A closer look at the DFMF requirements and deliverables levels reveals many similarities and concerns when compared with the categories and subcategories identified by DFOCC using grounded theory.

Tables 2 and 3 compare the DFMF requirements and deliverables against the DFOCC categories and subcategories. The similarities show that DFOCC, which is based on grounded theory, is consistent with

Table 2. Comparison of DFMF requirements and deliverables and DFOCC categories and subcategories.

DFMF Deliverable	**DFMF Requirement**	**Core Category**	**DFOCC Category**	**DFOCC Subcategory**
	Evidence handling and management policies	Policy	Facility building and management standards	Standards Best practices Guidelines Lab accreditation
	Incident management policies Education, training and awareness policies Management policies Infrastructure policies		Organizational policies	Information security policy Physical security policy Technology use policy Confidentiality and NDA Standards/accreditation
Evidence management Digital evidence Incident handling Investigation procedures	Evidence handling procedures Incident management procedures	Process	Investigation process	Scope of investigation Identification Preservation Analysis Reporting ACPO principles
BIA IRP DRP BCP New technologies	Risk mgmt/contingency procedures		Evidence admissibility	Data verif/validation Chain of custody Investigator qualifications Expert testimony Authentication
General management Use of forensics for non-forensics purposes Operational infrastructure	Management procedures Infrastructure procedures		Investigation procedures	Documentation Standard (ASCLD) Pre-investigation Case management Post-investigation

Table 3. Comparison of DFMF requirements and deliverables and DFOCC categories and subcategories (continued).

DFMF Deliverable	**DFMF Requirement**	**Core Category**	**DFOCC Category**	**DFOCC Subcategory**
	Code of conduct	People	Knowledge/background	Information technology
				Law
	Awareness programs		Education	Discipline
				Degree
Technical education and training	Education and training programs		Experience	Industry experience
First responder				Length of experience
Investigator				
			Training and development	Types of training
				Training as qualifications
Expert witness				Development
			Organizational hierarchy	Organization size
				Organization type
			Investigator traits	Investigative
				Communicative
				Technical
				Analytical
Intrusion detection	Operational infrastructure	Technology	Tools	Tool selection
Systematic gathering				Forensic software
Monitoring				Standard tools
Networks				Hardware
Time synchronization				Software/hardware
				Peripherals
				Small-scale devices
Hardware	Investigation infrastructure		Building a facility	Process
Software				Facility requirements
Miscellaneous				Financial
				Functionality/purpose
			Virtual environment	Cloud

some initial findings in the literature. This is especially true with regard to the multi-dimensional approach used to develop DFMF. The multi-dimensional approach was drawn from the information security domain, which von Solms called a multi-dimensional discipline [10]. Specifically, von Solms identified various dimensions for information security, including people, policy, risk management, legal, ethical, insurance, technology, strategic governance and operational governance. The dimensions were also used to develop an assessment model for information security using the corporate governance, people, policy, legal, compliance and technology dimensions. These dimensions create the similarities between DFMF and DFOCC.

Most significantly, the DFOCC core categories and the DFMF dimensions were created using different methods. DFOCC is based on grounded theory, which means that its core categories were derived by grounding the data throughout data analysis. DFMF, on the other hand, does not rely on such a systematic method; instead, it is derived from the literature in the multi-dimensional discipline of information security. In other words, the DFOCC is grounded in data, while the DFMF is not. In such a case, according to Jones and Valli [11], grounded theory "can furnish additional value when literature fails to support the theoretical evolution of phenomena." This makes the use of grounded theory in this research even more appropriate.

Although the goals, application and methodology of DFMF differ from those of DFOCC, DFMF actually validates DFOCC. This is because the DFMF dimensions and the DFOCC core capabilities focus on the same four areas: policy, process/investigation, people and technology/infrastructure. The strong correlations between the two frameworks, coupled with the multidimensional nature of the information security domain, demonstrate that DFOCC and DFMF lead to the same end point despite using different paths to get there. Indeed, DFMF and DFOCC both establish that digital forensic organizations must consider the four core capabilities when making decisions about digital forensics regardless of whether they are viewed from a management, development or investigation perspective.

3.4 Digital Forensic Laboratory Development

DFOCC provides a framework for sorting through a complete list of needs when developing a digital forensic organization. The financial constraints and scope of a digital forensic organization impact the extent to which the organization will adopt the set of capabilities in the books. As stated by Jones and Valli [11], the minimum requirements of a digital

forensic organization depends on factors such as the budget and scope of the organization's products and services. Jones and Valli also provide a "shopping list" of what an organization may or may not need according to its requirements. What is missing in the literature, therefore, is a guide on how to pick and choose the appropriate capabilities for a digital forensic organization to meet some minimum requirements. The difficulty, of course, is that the minimum requirements are subjective and highly dependent on the needs of an organization.

4. DFOCC Framework

DFOCC is a tool for building and managing the capabilities of digital forensic organizations. Note that DFOCC does not provide all the answers to developing and managing capabilities; such a task is beyond the scope of this research. Instead, the main goal of DFOCC is to make sense of the patterns identified in the data.

4.1 Equation Representation

DFOCC is based on an equation that concisely expresses the relationships in the data analyzed using grounded theory. The relationships between the four core categories are expressed using the equation:

$$C = P_1 \cdot (P_2 + I_1 + I_2) \tag{1}$$

where C denotes the capabilities of a digital forensic organization, $P1$ denotes policy, $P2$ denotes people, $I1$ denotes infrastructure and $I2$ denotes investigation. The equation was obtained using grounded theory, which involved the use of theoretical sensitivity and a conditional matrix, and grounding the theory in the data.

According to Equation (1), the capabilities of a digital forensic organization are obtained by multiplying policy (P_1) with the sum of people (P_2), infrastructure (I_1) and investigation (I_2). Thus, the capabilities cannot be achieved without policy. Policy is an overarching multiplier because each of the other three categories cannot exist without policies in place. Another consequence of using policy as a multiplier is that the equation can be expressed in partial terms as:

$$C = P_1 \cdot P_2 + P_1 \cdot I_1 + P_1 \cdot I_2 \tag{2}$$

This means that the core capabilities of people, infrastructure and investigation can be viewed separately, but each must be viewed with the policy multiplier. For example, it is not possible to have an infrastructure capability without policies in place that govern the use of software,

the maintenance of software, access control, etc. The same is true for the relationship of policy with the capabilities of people and investigation.

The DFOCC equations express several observations and statements about digital forensics and the development and management of the capabilities of digital forensic organizations. One of them is the definition of the capabilities of a digital forensic organization as the sum of the core capabilities of people, infrastructure and investigation governed by a comprehensive set of policies as a unique capability.

This definition of capabilities does not set a comprehensive minimum standard of capabilities for all digital forensic organizations. Instead, it requires all digital forensic organizations to consider the four core capabilities. For example, a digital forensic organization that does not have any policy governing people should not be considered capable regardless of the quality of the people and technology in the organization.

The following sub-equation expresses the comparative weight of the capabilities:

$$P_1 \cdot I_2 = P_1 \cdot P_2 + P_1 \cdot I_1 \tag{3}$$

where the addition of the capabilities of people and infrastructure equals the capabilities of investigation. In other words, investigation is the sum of people and infrastructure because people (digital forensic investigators and managers) use the infrastructure (hardware, software and laboratory) to conduct successful investigations. It is important to note that policy remains an important multiplier. A statement that can be derived from this sub-equation relates to investigation capabilities as follows: the capabilities of a digital forensic organization with regard to conducting digital forensic investigations are determined by the organization's capabilities with regard to people and infrastructure, each of which is governed by a set of policies.

The above statement is a subset of the previous statement regarding organizational capabilities. However, it is important to clearly delineate the difference between organizational capabilities and investigation capabilities. A digital forensic organization may be able to conduct digital forensic investigations, but it may not necessarily be a capable digital forensic organization. In other words, investigation capabilities can exist absent policies because the investigation process has frameworks in place that can account for the lack of a comprehensive set of policies. The organization's capabilities, on the other hand, cannot exist without comprehensive policies.

4.2 Role of Policy

The DFOCC framework suggests that policy must be present in all aspects of capabilities within a digital forensic organization. In particular, a digital forensic organization must have a set of policies in place that govern people, infrastructure and investigations in order to be considered digital forensics capable.

The role of policy at the organizational level has already been identified in the digital forensic readiness literature [17, 18]. Organizational policy, therefore, has played a significant role in the digital forensic readiness literature. Policy is also prominent in digital forensic standards, accreditation and best practices – International Standards Organization (ISO) standards, Association of Chief Police Officers (ACPO) guidelines in the United Kingdom and American Society of Crime Lab Directors (ASCLD) accreditation standards in the United States all incorporate policies in their processes. DFOCC states in clear terms that policy is a requirement for all the core capabilities; thus, organization capabilities cannot be achieved without policies. A set of policies must exist for people, infrastructure and investigations, regardless of how extensive the policy set may be. At the minimum, a digital forensic organization should consider adopting policies across the core capabilities that enhance the admissibility of evidence. An example of such a policy is access control, which bolsters the credibility and reliability of the entire organization as well as the resulting evidence. A starting point for such an inquiry is the essential requirements imposed by the American Society of Crime Lab Directors [2]. These essential requirements are standards that directly affect and have a fundamental impact on the work product of a laboratory and/or the integrity of the evidence [7]. The DFOCC framework and its equations lend themselves to further observations and statements about what it means to be a digital forensics capable organization in the context of development and management.

5. DFOCC Application

An important question is why DFOCC is important or even worth researching. Also, how exactly does DFOCC help digital forensic organizations? This section attempts to answer these questions and explain the applicability of the DFOCC framework to digital forensics. The DFOCC equations presented in the previous section can be applied to digital forensics in order to develop and manage digital forensic organizations. First, DFOCC can be used as a development tool to create a roadmap for building a digital forensic organization. Second, DFOCC can enhance evidence admissibility. Third, DFOCC can help improve the

efficiency and effectiveness of a digital forensic organization by improving management and going after areas of success. Finally, DFOCC creates a universal benchmark for organization capabilities that also takes into account small and consultancy-level digital forensic organizations.

5.1 Roadmap for Organization Development

No standard framework is currently available for building a digital forensic organization. This observation was corroborated in the survey data when the participants were asked: "Do you know any guideline for developing digital forensic [capabilities], a standard guideline?" The majority of the survey participants indicated that no industry standard exists for developing or managing digital forensic capabilities. Some participants did mention the Association of Chief Police Officers guide and the International Standards Organization and American Society of Crime Lab Directors standards and best practices. However, most participants noted that these are not directly related to developing and managing digital forensic capabilities.

DFOCC surpasses the work of Jones and Valli [11] in that it provides a framework for sorting through a complete list of the needs for developing a digital forensic organization. This is the same position taken by Jones and Valli as well as the International Standards Organization and American Society of Crime Lab Directors publications. In fact, according to the FBI [7], "the fact that a laboratory chooses not to apply for [ASCLD] accreditation does not imply that a laboratory is inadequate or that its results cannot be trusted." Jones and Valli provide a comprehensive "shopping list" of what a digital forensic organization may or may not need according to its requirements.

At this time, a guide is needed to help select the appropriate capabilities of a digital forensic organization that meet some sort of minimum requirements. The difficulty is that the minimum requirements are highly dependent on the needs of an organization [11]. The DFOCC framework provides a potential roadmap that can guide a digital forensic organization in its decision making process. The framework states that, in order to be able to conduct digital forensic investigations, there must be people, infrastructure and a set of policies for people, infrastructure and investigations. DFOCC does not say what the policies are because they still have to be determined by factors such as the organization's budget, size and scope. DFOCC, however, gives a digital forensic organization a good starting point in the decision making process and a way to express a benchmark for the capabilities using the equation:

$$C = P_1 \cdot (P_2 + I_1 + I_2) \tag{4}$$

5.2 Evidence Admissibility

The DFOCC policy multiplier likely encourages digital forensic organizations to be more aware of the pitfalls of evidence admissibility. The survey participants stated that some reasons for the inadmissibility of digital forensic evidence were: (i) qualifications of digital forensic experts; (ii) authenticity of evidence via an unbroken chain of custody; and (iii) preservation of digital forensic evidence during investigations. Evidence likely becomes inadmissible because a digital forensic organization lacks the policies needed to ensure that the process it used satisfied the minimum threshold for admissibility.

The reasons for evidence becoming inadmissible can be connected to the DFOCC framework. For example, the qualifications of a digital forensic expert fall under the $P_1 \cdot P_2$ category, where digital forensic organizations ought to set a standard for educating and qualifying individuals as digital forensic experts, an issue that surprisingly is constantly debated in the discipline. Under the $P_1 \cdot P_2$ category, DFOCC would require a digital forensic organization to identify the qualifications of all its personnel. The digital forensic organization would have to create policies that cover the education and qualifications of its people. The lack of these policies and stated minimum requirements for qualifications would mean that a digital forensic organization does not have the requisite capabilities under DFOCC.

The chain of custody issue falls under the $P_1 \cdot I_2$ category of DFOCC, which requires organizations to create a documented policy for establishing chain of custody, a practice that is fortunately common in the discipline, but has not become a minimum standard for all digital forensic organizations to follow and for which all digital forensic organizations do not implement policies, as evidenced by the survey data. The lack of documented processes would mean that a digital forensic organization would not be deemed capable under DFOCC.

With regard to the preservation of the evidence during an investigation, the DFOCC framework would require the examination of an organization's evidence preservation practices, including the tools used and the processes followed to preserve the evidence. The tools should be accepted by the discipline as standard practice for preservation and digital forensic organizations should have policies in place that require the use of the tools to meet DFOCC capability requirements. The absence of tools for preserving evidence would mean that the digital forensic organization would not be deemed capable under the DFOCC framework. In other words, following the DFOCC framework would mean that a digital forensic organization has the minimum capabilities. Thus, the

Table 4. Sample application of the formula: $C = P_1 \cdot P_2 + P_1 \cdot I_1 + P_1 \cdot I_2$.

Policy and People ($\mathbf{P_1 \cdot P_2}$)	**Policy and Infrastructure** ($\mathbf{P_1 \cdot I_1}$)	**Policy and Investigation** ($\mathbf{P_1 \cdot I_2}$)
People capabilities (more detailed than $P_1 \cdot I_1$ and $P_1 \cdot I_2$)	Infrastructure capabilities (less detailed than $P_1 \cdot P_2$)	Investigation capabilities (less detailed than $P_1 \cdot P_2$)
People policies (more detailed than $P_1 \cdot I_1$ and $P_1 \cdot I_2$)	Infrastructure policies (less detailed than $P_1 \cdot P_2$)	Investigation policies (less detailed than $P_1 \cdot P_2$)

digital evidence offered in court by a DFOCC-compliant organization would likely have a higher rate of admissibility.

5.3 Areas of Success

Another potential application of the DFOCC framework is to help identify areas of success in a digital forensic organization. Specifically, a digital forensic organization can use DFOCC to test whether perceived key factors of success match the organization's digital forensic capabilities. This can be done by first identifying a key success factor (e.g., quality of its people).

Next, the digital forensic organization must list all its digital forensic capabilities according to the DFOCC equation and examine if its capabilities match its key success factor. Table 4 shows how this works. The organization categorizes its capabilities according to the DFOCC equation by listing its people capabilities and people policy under the $P_1 \cdot P_2$ category, then its infrastructure capabilities and infrastructure polices under the $P_1 \cdot I_1$ category, and then its investigation capabilities and investigation polices under the $P_1 \cdot I_2$ category.

If the key success factor is really the quality of its people, then the list of people capabilities and people policies under the $P_1 \cdot P_2$ category would be comparatively more comprehensive and detailed than the $P_1 \cdot I_1$ and $P_1 \cdot I_2$ categories. The DFOCC framework potentially gives digital forensic organizations a systematic and simplified methodology for analyzing their capabilities and policies, and how the capabilities and policies relate to each other. Additionally, a digital forensic organization could perform comparisons across policies and, thus, create higher-level policies that cut across and unify the organization, possibly enhancing cohesion in the organization's processes.

5.4 Attainable Universal Benchmark

An important application of DFOCC is providing smaller organizations, even individual digital forensic consultants, with a means to create organizational benchmarks without undergoing a more expensive accreditation process. As one survey participant explained: "I don't believe you need to be accredited to [ISO] 27001 or 17025. I think those are good, but they're optional. They're a big burden. They are both ... big financial burdens."

Although additional data and research are needed to realize this potential, the DFOCC framework could serve a basis for identifying common benchmarks in digital forensic organizations that can be implemented without the burden of accreditation. For example, the survey reveals that the majority of participants use FTK from Access Data and/or EnCase from Guidance Software as their forensic analysis software. In other words, these two tools have become standard in the discipline. One survey participant stated the choice to use FTK and Encase as follows: "They are the industry standards. Everyone uses them, so we have to be able to read and write in their formats." Such observations could be established using quantitative research into digital forensic capabilities that leverages the DFOCC framework.

5.5 DFOCC Advantages

The DFOCC framework offers advantages in comparison with existing best practices and guidelines. First, the framework is simple and comprehensive. The framework narrows everything down to four variables: (i) policy; (ii) people; (iii) infrastructure; and (iv) investigation. Also, it can be expressed in equation form, which simplifies the expression of the relationships between the core capabilities as discussed above.

Another key advantage of DFOCC is that it is interconnected. The DFOCC equations recognize the interconnectedness of the core capabilities and policy acts as an adhesive for all the capabilities. Further, the survey data reveals that the interconnectedness also emerges in the category, subcategory and phenomenon levels. An example is the number of investigators (this corresponds to a dimension) that are needed in a laboratory. This issue initially affects the core people category by playing a key role in determining the scope and size of an organization. The same dimension, however, also appears in the investigation process with regard to the number of investigators needed to create a peer review system in a digital forensic investigation. The number of investigators also affects decisions regarding the infrastructure because the number of people in an organization is a factor in budgeting and creating software,

hardware and facility requirements. Finally, the number of investigators affects policy because policies have to be specified for hiring and retaining people, performing validation and verification, and ensuring infrastructure efficiency.

Another advantage of the DFOCC framework is that it acts in a multilevel manner by considering the different types, sizes and scopes of digital forensic organizations. The framework could be applied to an individual as long as the individual has identified minimum benchmarks for each of the core categories using DFOCC. Finally, the formulation of the DFOCC framework using grounded theory is important; this ensures that the core categories and core capabilities are firmly grounded in data and that the data leads the application of the framework.

6. Conclusions

The DFOCC framework is designed specifically for building and managing the capabilities of digital forensic organizations. The framework employs equations that express the relationships between core capabilities, enabling the definition of digital forensic capabilities. The reliance of DFOCC on grounded theory means that the abstract notions of its core categories are themselves grounded in the data. Most importantly, the framework is also grounded in the literature on digital forensic capabilities, specifically research on digital forensic readiness, capability maturity models, digital forensic management frameworks and best practices for building and managing digital forensic laboratories. Therefore, the DFOCC framework is readily integrated with other theories; indeed, it identifies gaps existing in the theories and also provides opportunities to extend the theories.

References

[1] E. Al-Hanaei and A. Rashid, DF-C2M2: A capability maturity model for digital forensic organizations, *Proceedings of the IEEE Security and Privacy Workshops*, pp. 57–60, 2014.

[2] American Society of Crime Lab Directors/Laboratory Accreditation Board, Accreditation Programs, Garner, North Carolina, 2016.

[3] E. Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*, Academic Press, Waltham, Massachusetts, 2011.

[4] J. Corbin and A. Strauss, *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*, Sage Publications, Thousand Oaks, California, 2008.

[5] J. Creswell, *Research Design: Qualitative, Quantitative and Mixed Methods Approaches*, Sage Publications, Thousand Oaks, California, 2014.

[6] T. Ellis and Y. Levy, Towards a guide for novice researchers on research methodology: Review and proposed methods, *Issues in Informing Science and Information Technology*, vol. 6, pp. 323–337, 2009.

[7] Federal Bureau of Investigation, The accreditation decision, *Forensic Science Communications*, vol. 1(1), 1999.

[8] B. Glaser and A. Strauss, *The Discovery of Grounded Theory: Strategies for Qualitative Research*, Aldine Transaction, New Brunswick, New Jersey, 2009.

[9] C. Grobler, A Digital Forensic Management Framework, Ph.D. Thesis, Department of Informatics, Faculty of Science, University of Johannesburg, Auckland Park, South Africa, 2011.

[10] C. Grobler and B. Louwrens, Digital forensics: A multi-dimensional discipline, *Proceedings of the Information Security South Africa from Insight to Foresight Conference*, 2006.

[11] A. Jones and C. Valli, *Building a Digital Forensic Laboratory: Establishing and Managing a Successful Facility*, Butterworth-Heinemann and Syngress Publishing, Burlington, Massachusetts, 2009.

[12] M. Kerrigan, A capability maturity model for digital investigations, *Digital Investigation*, vol. 10(1), pp. 19–33, 2013.

[13] P. Martin and B. Turner, Grounded theory and organizational research, *Journal of Applied Behavioral Science*, vol. 22(2), pp. 141–157, 1986.

[14] M. Pollitt, An ad hoc review of digital forensic models, *Proceedings of the Second International Workshop on Systematic Approaches to Digital Forensic Engineering*, pp. 43–54, 2007.

[15] C. Robson, *Real World Research*, Blackwell Publishers, Malden, Massachusetts, 2002.

[16] R. Rowlingson, A ten-step process for forensic readiness, *International Journal of Digital Evidence*, vol. 2(3), 2004.

[17] R. Rowlingson, An Introduction to Forensic Readiness Planning, Technical Note 01/2005, National Infrastructure Security Coordination Centre, London, United Kingdom, 2005.

[18] C. Taylor, B. Endicott-Popovsky and D. Frincke, Specifying digital forensics: A forensics policy approach, *Digital Investigation*, vol. 4(S), pp. S101–S104, 2007.

[19] A. Valjarevic and H. Venter, A comprehensive and harmonized digital forensic investigation process model, *Journal of Forensic Sciences*, vol. 60(6), pp. 1467–1483, 2015.

[20] S. von Solms, C. Louwrens, C. Reekie and T. Grobler, A control framework for digital forensics, in *Advances in Digital Forensics II*, M. Olivier and S. Shenoi (Eds.), Springer, Boston, Massachusetts, pp. 343–355, 2006.