# DF-C²M²

# A Comprehensive Capability Maturity Model for Digital Forensics Organisations

**Ebrahim Hamad Salem Al Hanaee**

MSc (Distinction) Information Technology (Zayed University, UAE, 2011)
MSc (Distinction) Computer Based Information System (Sunderland University, UK, 2000)

Computing Department
Lancaster University
United Kingdom

Submitted for the Degree of
Doctor of Philosophy

October 2016

# Declaration

I declare that this thesis has been written by myself, and the work reported herein is my own account of my research. The work reported in this thesis has not been previously submitted in substantially the same form for the award of a higher degree elsewhere.

***Ebrahim Hamad Salem Al Hanaee***

# Acknowledgements

My first and foremost thanks and praises are due to Allah (God) Almighty who has helped me and provided me with faith, patience and commitment to complete this research.

I would like to express my sincere gratitude to my supervisor, Prof. Awais Rashid, for his unfailing support, encouragement and willingness to provide constructive feedback on my ideas – I could not have completed this thesis without him.

Special admiration and gratitude are due to my parents, wife, brothers and sisters whose prayers, love, care, patience, support and encouragement have always enabled me to perform to the best of my abilities.

Last but not least, special thanks are due to all those who took part in the assessment and evaluation process for the new proposed model. I would like to thank all the people, members of my family and close friends, who have borne with me during the period of my PhD studies.

# Abstract

The field of digital forensics has grown from an obscure area of interest amongst computer enthusiasts to become an emerging forensic scientific discipline of great significance in criminal investigations and civil litigations across the globe. The majority of digital forensic laboratories today are faced with ever-increasing legal and regulatory demands to meet internationally accepted rules regarding the admissibility of digital evidence, as well as being faced with various pending regulatory mandates requiring international accreditation of digital forensic facilities. These two major requirements, coupled with ever-increasing case backlogs and limited resources, have left many digital forensic labs to confront what initially seems to be an 'insurmountable challenge' to manage their caseloads, implement new regulatory requirements, and still find ways to improve overall efficiency and effectiveness.

Based on the Capability Maturity Model (CMM) paradigms, the Digital Forensics - Comprehensive Capability Maturity Model (DF-C$^2$M$^2$) was born out of the findings of this research and the scientific gap that exists in the current digital forensics standards, best practices, frameworks, and models. This model has been developed through consultations and interviews with digital forensics experts.

The DF-C$^2$M$^2$ enables the measurement of maturity along three key organisational dimensions: people, processes, and tools, while enabling such an assessment to be tailored to a particular type of organisation, e.g., law enforcement or non-law enforcement. The inclusion of capability maturity across multiple key domains is designed to provide a more comprehensive capability maturity assessment of an organisation – across its three inter-dependants 'influencer' domains, when compared with other capability maturity models that focus on only specific domains such as processes, or on a sub-element of a domain.

The model has been tested and evaluated as a management support and Capability Maturity Assessment system within two labs. One of the labs is an ISO 17025 accredited digital forensic lab within a law enforcement agency, while the other one is a non-accredited lab within an academic institute.

The model will also serve as a stepping stone towards a timelier, more effective, and more efficient means of developing and implementing digital forensic standards and best practices moving forward.

In summary, the DF-C$^2$M$^2$ was designed to address the cited challenges by creating a modular management decision support framework to enable labs to better manage and achieve their objectives through a system of assessments and planning tools all geared towards measuring compliance and Capability Maturity across multiple domains.

# Table of Contents

# List of Tables

# List of Figures

# CHAPTER 1: INTRODUCTION TO THE RESEARCH

## 1. 0 INTRODUCTION

Across the developed world, in instances where credible, irrefutable digital evidence is produced by the prosecution, it is not uncommon for defence attorneys to try to attack the credibility of the digital forensics examiner, their digital forensic laboratory processes, and their technical records, reports, and any related conclusions (Krause, 2010). 'If doubt is cast on the initial collection and management of evidence, output from the other phases is moot' (Tipton & Krause, 2007) as the evidence derived from such processes may later be challenged or questioned as being non-irrefutable by the courts and could adversely affect the outcomes of both civil and criminal cases that depend on such evidence.

In 2001 at the DFRW conference titled: A Roadmap for Digital Forensics – Big Computer Forensic Challenges", Dr Eugene Spafford identified a gap that Academic research in support of government and commercial endeavours often focuses on technological results. "Research must address challenges in the procedural, social, and legal realms as well if we hope to craft solutions that begin to fully "heal" rather than constantly "treat" our digital ills" (Spafford, 2001 ). Spafford went on to identify what he believed to be the key components of a more holistic approach to research related to digital forensics.

Spafford listed the major challenges as being; keeping up with technology advances, the need for standardised analytical procedures and standardised terminologies within digital forensics, developing tools and methods that comply with legal/regulatory requirements, training and more intuitive tools to help address skills deficiencies. Spafford also called for greater accuracy and more reliability in Digital Forensics tools and methods.

Increasingly, there is a requirement from the various legal and judicial authorities throughout the world that any digital evidence presented in criminal and civil cases should meet the requirements of Daubert or Frye regarding the acceptance and admissibility of digital evidence (Kessler, 2011). To date, digital forensics labs that have implemented a quality management system with the view of gaining international accreditation have mostly done so by adopting and implementing the ISO/IEC 17025:2005 standard or the US equivalent ASCLD-LAB International Requirements.

The drive towards ISO 17025 accreditation has largely been motivated by regulatory requirements. Within the European Union Article 12 of Regulation (EC) No 882/2004 (EU Parliament, 2004), to be designated as a 'recognised laboratory', laboratories have to be accredited in accordance with EN ISO/IEC 17025 on general requirements for the competence of testing and calibration laboratories. Additionally, the EU states that there is a need to '… define commonly accepted minimum forensic science standards for the collection, processing, use and delivery of forensic data relating inter alia to data …., and to equip the Union to meet the new challenges that it is facing in the field of high tech and cybercrime' (EU PARLIAMENT, 2004). Consequently, in the absence of any defined accreditation standards for digital forensics labs, ISO 17025 and similar standards are being adopted (rather than adapted) to address the need for standardisation and accreditation along with some well-intended best practices and country-specific legal requirements (where applicable). International standards such as ISO 17025 may be viewed by some organisations as a panacea to solving digital forensics process maturity, and improvement processes, however, their suitability and practicalities (shortcomings and pitfalls) as they are applied specifically to the discipline of digital forensics are often overlooked due the lack of a viable, reliable alternative.

Beebe argues that digital forensics has grown from an obscure niche area of scientific interest amongst computer enthusiasts to become an emerging forensic scientific discipline of great significance in criminal investigations and civil litigations across the globe (Beebe, 2009). Internationally, as an increasing number of civil and criminal investigations have required joint cooperation between multiple forces and judiciaries, the need for international acceptability of digital evidence has grown, and therefore so too has the need for international accreditation, as a basic means of quality assurance related to digital evidence examinations. However, it is vital that the standards implemented are fit and suited for purpose and not just an amalgamation of various legacies, traditional scientific standards, and best practices that do not always translate or necessarily apply to the field of digital forensics. Perhaps more importantly, whilst ISO 17025 accreditation is a goal to which many digital forensic labs aspire to, far more labs are faced with a more pressing and tangible business needs to accurately assess their capability maturity and continuously improve it, for greater business and personnel efficiency.

ISO 17025 was designed as a quality management standard for testing and calibration laboratories and includes quality management, and competency and proficiency testing of personnel as its key elements. ISO 17025 is best suited to the testing of physical artefacts, where the results are generally empirical and categorised as either being positive or negative, and the testing methods for each type of test and artefact are very well-defined, subject to some variations, and not subject to multiple possible interpretations of the results. In contrast, Digital Forensics is a comparatively new and ever-developing scientific field with a variety of unique nuances, tools, methods, and means of interpretation of results where the goals of digital forensic examinations are often performed to help prove or disprove a hypothesis, and the findings may be subject to multiple interpretations.

In the absence of a bespoke alternative to address quality management, and competency and proficiency testing within digital forensic laboratories, ISO 17025 has been adopted as the 'accepted' or 'de facto' standard for digital forensic laboratories seeking international accreditation.

In parallel, international efforts towards global unification of cybercrime laws and conventions have made significant progress to date within the European Union (EU) and Gulf Cooperating Countries (GCC). However, trans-national criminal investigations and successful prosecutions would be ineffective without a framework of an internationally accepted digital forensic framework of standards (covering digital evidence handling, examination, analysis, and evidence exchange) that could easily be implemented across national boundaries and that would address the practicality, cost, and timeliness (relevance) requirements that law enforcement agencies are requesting.

The first international standards related to digital forensics such as ISO 27037:2012 and various draft international standards related to digital forensics analysis may in the future assist in addressing some of the areas for standardisation, but will still fall short of providing a more holistic and modular (extensible) framework that enables organisations to address their current and future requirements for an efficient, quality-driven digital forensic lab.

The need for a modular framework is highlighted by the fact that various (current and future) standards and best practices that apply to digital forensics may (in future) need to be integrated (based on regulatory requirements) into a unified framework through which a digital forensic lab can effectively manage its required standards and regulatory requirements such as digital evidence handling, analysis of digital evidence, and business process-related frameworks such as business continuity. The ability to integrate all of these requirements into a unified framework, rather than a collection of separately managed ones, will enable more effective utilisation of resources, promote a better understanding of process inter-relationships, and allow the organisation to measure its capability across all domains and standards within a unified management framework.

Furthermore, whilst ISO standards (in general) are viewed as quality management improvements that will, in theory, lead to greater business efficiency and thereby maturity, none of the existing ISO standards attempt to address the pressing business and operational needs for establishing, measuring, and improving digital forensics capability maturity.

Although the perceived benefits of ISO accreditation may vary between labs, decision-makers, and practitioners, organisations today are evaluating how to streamline processes to achieve optimal process efficiency and throughput. These preceding items are the key factors that determine the long-term operational costs, case backlogs, quality improvement, capacity building, and overall customer satisfaction for these labs. ISO 17025 accreditation is often a secondary business driver or requirement for many digital forensic laboratories.

Operational efficiency is often primary business goal and objective, and there is a need to provide digital forensic organisations for a cost-effective, up-to-date, and relevant ‘enabler management support systems’ or frameworks; that enable them to effectively implement their regulatory and standards requirements, in addition to finding effective means to measure, benchmark, and improve their overall capability.

## 1.1 BACKGROUND

Of the many digital forensic models and frameworks developed to date, the majority of these have focussed on investigative processes, tools, or methods, and none provide digital forensic labs with a simple and yet rigorous mechanism to evaluate their process effectiveness or capabilities and plan a roadmap to improve in an easy and effective manner.

Digital forensic labs are facing a plethora of challenges related to technology changes, the constant need for skills to be updated and re-assessed, a mix of best practices, ad-hoc methods, and standards to follow.

"Digital forensic investigations are becoming more complex due to the increasing size of digital storage… new approaches for managing the case details of a digital forensics investigation must be developed" (Dampier T. a., 2010). In 2006 at the DFRWS conference, in the presentation "Challenges in Digital Forensics" (Lindsey, 2006) FBI Director Ted Lindsey identified several challenges in Digital Forensics.

The key challenges presented by Lindsey related primarily to rapidly changing and new technologies, increased volume of evidence (due to increased device storage capacity, virtualization and the use of encryption and rise in anti-forensic (tools). These challenges could be summarised as "technological challenges" facing digital forensic investigations. Ironically, the majority of the challenges and concerns first voiced over a decade ago are still relevant and applicable to challenges today in digital forensics.

The result is that digital forensic labs are mostly left with costly piecemeal efforts in order to try and address their pressing legal, regulatory, technical, and business requirements independently with little opportunity for assessing their current posture and measuring their conformance with requirements, and lacking the ability to assess their maturity levels across all aspects of their business operations.

Presently, no framework/model exists that would allow a lab to assess its current posture regarding:

- Regulatory and standards compliance,
- Capability maturity, across People, Process and Tools domains.
- What does it need to do to improve?

- What is it doing well?
- What is it not ineffectively? and
- Plan a roadmap to effectively address present issues.

In view of the vast array of challenges and backlogs faced by digital forensics laboratories, it can be argued that digital forensics capability maturity is now a necessary, overlooked aspect of digital forensics quality management that has been identified as an essential business and quality assurance requirement that merits further research and effort to establish a sustainable model and framework for implementing and managing it. Digital forensics capability maturity can be applied to a multitude of organisations, regardless of size, regulatory requirements, scope of services, and accreditation status.

### 1.1.1 General ISO Standard Limitations as they apply to Digital Forensics

ISO 17025 is a general standard of quality assurance for testing and calibration laboratories and as such, ISO 17025 does not consider various characteristics of digital forensics testing (examinations) including:

- As a standard designed to test and calibrate laboratories, ISO 17025 has proven to be good at helping enforce a quality management system and basic competency management system within digital forensic labs, but it may be viewed by some as being costly (time and resources) to implement and maintain within a digital forensic laboratory in view of the additional processes and related overheads that would need to be implemented to be compliant.
- Requirements such as the need within ISO 17025 to define the documented test methods used for a particular test (examination) within the test report and any measures of uncertainty simply do not easily translate to the discipline of digital forensics.
- ISO 17025 works well in empirical test environments where the possible outcomes are clearly defined and can be measured. Digital forensics examinations and requirements do not lend themselves as easily to the same rules and requirements. In the majority of scientific testing scenarios that ISO 17025 was designed for and caters to in labs whose results are based on empirical results, test equipment is calibrated prior to the start of each test. Digital forensics, by the very nature of computing, does not easily lend itself to such criteria, and more

needs to be done to adapt ISO 17025 to what is practical and realistic for digital forensics.

- Although ISO 17025 requires annual [1] proficiency testing of examiners for all types of tests conducted within a lab's scope of accreditation - no external proficiency tests existed for mobile phone forensics until recently.

While ISO 17025 provides a foundation and a minimum set of requirements as a starting point that can be applied to digital forensic labs, it was not designed to address the vast majority of business, technical, and efficiency challenges of an active digital forensic lab. ISO 17025 does not factor in capability maturity requirements across the people, process and tools requirements, nor is it well-suited cater to for technical differences in processes, and interpretations of data when comparing between traditional scientific versus digital forensic examinations processes.

ISO 17025 is not a panacea to solving digital forensic standards, maturity and capability issues that it is sometimes misinterpreted to be, and more needs to be done to augment the current applied standards and enable organisations to effectively tackle and manage the capability maturity, and compliance issues that they face today.

### 1.1.2 Existing Digital Forensics Models

The majority of academic literature related to digital forensics generally focuses on newer investigative processes, steps, and tools, and does not address the issues of measuring and managing compliance, or decision support, nor does it address the need for capability maturity and methods for capability maturity assessments.

Within the past decade, several digital forensic investigation models have been published (Agarwal, Saurabh, & Gupta, 2011). Many of these models have been designed and proposed to address process methods and alternatives; these include:

- Kruse and Heiser Model (Heiser, 2002).
- Department of Justice (USDOJ) - Forensic Process Model (Justice U. D., 2004).
- Casey's (Yale) Model (Casey, 2004).
- DFRWS framework meta-model (DFRW, 2001).
- The Ciardhuain model (Ciardhuain, 2004).

[1] Proficiency test frequency is subject to accreditation body's requirements. In some instances, this frequency may be at least per accreditation cycle.

Each of the above models defined a number of unique steps or stages related to digital evidence handling, examination, and storage. Some extended their model to cover elements of investigation, planning, review, and reporting, but none extended their models to look at issues related to capability maturity, efficiency, integration with international standards, or quality management processes. Each focussed on a specific technical aspect related to digital forensics, with none of the models or frameworks assessing digital forensics from a holistic quality management and technical perspective.

Addressing technical issues (tools) in digital forensic models, without addressing non-technical issues related to other key domains such as People, and Processes including capability maturity, standards, and regulatory requirements seems to be a common pitfall of many of the digital forensic models and frameworks proposed to date.

The vast majority of research and development within the field of digital forensics has focussed on developments in technology. These research projects have tended to focus largely on addressing how to best extract and examine evidence from new technologies, or on training and certification. Very little, if any, of the current research has begun to look at efficiency, quality, integration with standards, shortcomings in present standards, and capability maturity within the scope of digital forensics – nor how to effectively measure compliance within the model across all elements (people, process and tools), in conjunction with related standards and best practices.

Two digital forensics-related models that explore, to some degree, the requirements for capability maturity are the Computer Forensics Capability Maturity Model (CF-CMM) (US Patent No. 2006/0069540 A1, 2006) and the Digital Investigations Capability Maturity Model (DI-CMM) (Kerrigan, 2013).

The Computer Forensics-Capability Maturity Model (CF-CMM) is essentially a ‘Methodology for assessing the maturity and capability of an organization’s internal computer forensic processes’. The CF-CMM presents a method for applying CMM to generic computer forensic processes and for conducting a Computer Forensics CMM Assessment (CFAM).

Essentially, the CF-CMM presents a method to categorise processes used internally within an organisation by looking at their forensic architecture and processes. It is designed for use within internal organisations that provide forensic services to internal customers and systems, and could be considered to be part of an organisation's internal computer forensics readiness assessment. CF-CMM does not address other key aspects of digital forensics such as people, tools, and compliance and integration with standards and regulatory requirements.

The Digital Investigations Capability Maturity Model (DI-CMM) (Kerrigan, 2013) focuses, in contrast, on five generic groupings of tasks associated with digital investigations; namely: Pre-process, Acquisition and Preservation, Analysis, Presentation, and Post-process. The DI-CMM focusses on the broader subject of digital investigations from start (Pre-process) to completion (Post-process), an element of which (Analysis) may include examination of digital forensic artefacts, but it is not geared towards focussing exclusively on the specialist area of digital forensics or digital forensic labs.

Although the DI-CMM includes general overviews of three key elements – People, Process and Tools – it does not address the capability maturity requirements of each, nor does it provide any tools to measure and address any areas of deficiency within the organisation, or provide recommended approaches or plans for addressing any deficiencies.

Likewise, unlike other scientific testing fields that have a well-established repository of information, knowledge bases, and best practices that are well-documented and accepted by the industry of practitioners, additionally  digital forensics-specific standard operating procedures are seldom shared within the community of practitioners, and validation and vetting of such procedures is often left to the discretion of the individual labs and their implementers (Al_Hanaee & Rashid, 2014).

## 1.2 PROPOSED APPROACH

The scope of the research was to examine three key organisational components of a digital forensic lab with the view of determining if the requirements for each area were adequately addressed at present. Areas for improvement, and tools to enable assessments and improvement in each key area were also identified during on-site assessments and reviews of the existing accredited lab. The three key organisational areas that were included within the scope of the research are: People, Process, and Tools.

This research proposes a comprehensive digital forensics capability maturity assessment and decision support model that addresses three key organisational sub-domains: People, Tools, and Process as shown in Figure 1, and integrates with existing digital forensics quality management standards ISO 17025 and best practices requirements.

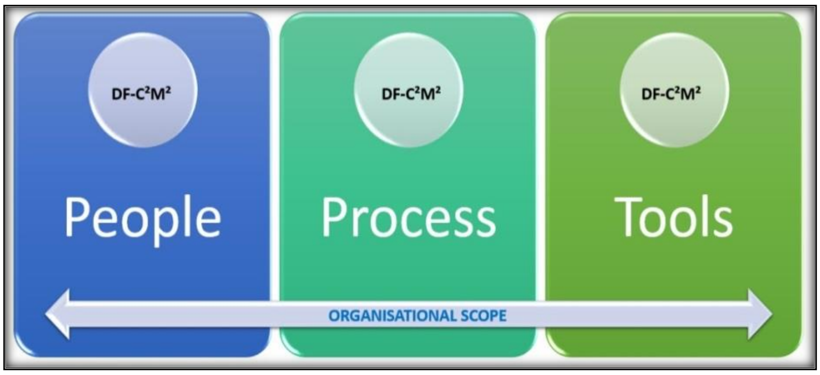


**Figure 1: DF-C$^2$M$^2$ key elements**

The Digital Forensics - Comprehensive Capability Maturity Model (DF-C$^2$M$^2$) provides a method to define, assess, and measure maturity levels and ISO 17025 compliance across the digital forensic lab, and a feedback and rating system to allow organisations to plan for improvement and (collectively) to benchmark their maturity level against other benchmarks.

The DF-C$^2$M$^2$ was born out of the findings of this research, and its design goal was to create a reliable, readily accessible modular framework that would enable an organisation (regardless of its present size or capability) to successfully implement a set of digital forensic standards, and to create a baseline upon which the organisation could be measured.

The model addresses the capability maturity and quality management requirements of three key organisational domains: People, Process, and Tools, and their inter-relationships.

The DF-C$^2$M$^2$ model is supported by a tool that enables an organisation to:

- Assess and measure its digital forensics capability and its maturity,
- Plan digital forensic services pertaining to People, Tools, and Processes,
- Quickly utilise a knowledge base and repository of procedures, policies, forms, and validated test methods,
- Determine skills requirements and personnel skills profiles,
- Implement training and corrective actions, and
- Plan and monitor improvements.

The DF-C$^2$M$^2$ tool provides a menu to allow the assessor to tailor assessment the requirements to suit a particular organisation type, e.g. a typical digital forensics laboratory as supported under ISO 17025/ASCLD-LAB scopes of accreditation within law enforcement (LE), and non-LE organisations, etc. For each organisation type, a Service Catalogue of planned or proposed services is provided. The idea for a Service Catalogue that lists services available and limitations was derived from a previous project, where as Director of a Police Station, the researcher had created a service catalogue was created for the public detailing services available to them and the requirements to use each service. For each the prerequisites for the delivery of each service were defined together with any applicable limitations are service level targets.

The DF-C$^2$M$^2$ Service Catalogue took the same concept to a much more detailed and granular level as a planning and readiness tool. The idea to categorise services based on lab units within a lab was based on the structure the researcher had previously created as part of a digital forensic lab project. Service Categories such as Live & Network Forensics and Digital Evidence Handling was based on input from practitioners involved in various aspects of the project. Cybercrime analysis was based on survey participant feedback.

The DF-C$^2$M$^2$ Service Catalogue covers a broad range of digital forensic-related services in several categories, namely:

- Computer Forensics,
- Mobile Device Forensics,
- Digital Audio Forensics,
- Digital Video Forensics,
- Live and Network Forensics,
- Cybercrime Analysis services, and
- Digital Evidence Handling Support services.

These categories of services cover the vast majority of services that the typical law enforcement digital forensics labs or units may be required to provide to the customer base. From a strategy and planning perspective, the Service Catalogue may also serve as a roadmap of which services a digital forensics lab would like to implement over e.g. a three-year plan, and identify which services from the list are essential to the unit's goals, objectives, and success, and which services should be considered as optional. Based on the Service Catalogue, an organisation would be able to more effectively design a roadmap for implementing these services.

Furthermore, by identifying the process, tools, and skills requirements for each service, the organisation can more accurately determine the costs for implementing such services and the relative value of each planned service, and factor in the most pressing demands and requirements from the customer base.

The creation of the DF-C$^2$M$^2$ based on a modular design was to allow for extensibility, enabling additional standards and practices to be incorporated, and to allow easier updates and revisions as may be required. Based on the Capability Maturity Model (CMM) paradigms, this model is aimed at enabling organisations to measure their maturity, and identify and prioritise areas for improvement, enabling organisations to establish a baseline for measurement, and to build roadmaps for future improvements to reach their required capability maturity levels across multiple domains.

## 1.3 NOVEL ASPECTS

The main contribution of this thesis is to develop a comprehensive digital forensics model (DF-C$^2$M$^2$) based on the Capability Maturity Model (CMM) paradigm. In addressing gaps within the current school of thought, and standards and frameworks related to digital forensics, the model enables the measurement of the level of maturity of an organisation with regards to digital forensics techniques, practices, tools, and processes.

The novel aspects of the DF - C$^2$M$^2$ model are as follows:

- The model would enable measuring maturity along three key organisational dimensions- people, processes, and tools - while enabling such an assessment to be tailored to a particular type of organisation, e.g., law enforcement (in support of criminal investigations) or non-law enforcement (in support of civil litigations and information security incident response) setting. Both law enforcement and non-law enforcement digital forensic laboratories would typically be geared towards different rules of evidence (Civil versus Criminal), and have their internal processes and designed to cater for such.
- The model would provide a management support and evaluation tool supplemented by a knowledge base of standard operating procedures, workflows, tests, and technical guides, which would enable organisations to measure their digital forensics capability maturity and identify roadmaps for improvement.
- The knowledge base includes a detailed services planning tool referred to as the Service Catalogue that would enable organisations to examine which services of the fifty-four defined services it needs to provide, how to prioritise implementation of the services, and understand the underlying prerequisite requirements (People, Process, and Tools) in order to effectively plan, enhance, or deliver the various services identified.
- The model provides fully functional, ready-to-use planning and assessment tools, enabling digital forensic laboratories to implement the core accreditation requirements equivalent to ISO 17025 but adapted and designed to specifically suit the realm of digital forensics, with the benefit of industry practitioners' acceptance and shared best practices.

The DF-C$^2$M$^2$ is not designed as a replacement or a new standard related to digital forensics laboratory management, but rather as a digital forensics management decision support and process improvement model.

## 1.4 RESEARCH METHODOLOGY

Due to the novel aspects of this research, and the need to conduct analysis of the use of existing standards and processes, the Design Science Research Process (DSRP) (Peffers, et al., 2006) was selected as the core research methodology. DSRP was found to be a more pragmatic research method and lends itself easily to understanding and measuring performance-related topics from personnel to processes. The selection of Design Science rather than alternatives such as Requirements Engineering (Nuseibeh & Easterbrook, 2000) was made on the basis that it is particularly suited to the task of creating a new process model.

In keeping with the core research and design ethos of 'by practitioners for practitioners' or participatory design (Murphy & Hands, 2012), the goal of the research methods was rooted in a comprehensive online survey of digital forensics experts in private labs and in law enforcement agencies as well as direct interviews with such experts, and assessments of both accredited and non-accredited digital forensic laboratories. Furthermore, the model would also draw upon the author's practical experience of working in digital forensics labs or settings involving digital forensics.

### 1.4.1 Problem Identification and Motivation

One of the main objectives of this research is to assess, evaluate, and design a comprehensive digital forensics model based on the Capability Maturity Model (CMM) paradigm, which would allow for establishing a mature profession in the area of digital forensics. The overall goal/objective is to improve the quality and maturity of digital forensic labs, through the integration of capability maturity with other pressing business and regulatory requirements in the form of tools and guides.

In order to help fulfil the overall goal of this research stakeholder /practitioner input would be essential. Critical to this research is to explore: the present challenges and requirements of a law enforcement agency's digital forensic laboratory, the practical requirements and limitations to achieving accreditation and operational efficiency, and to defining and understanding digital forensics skills requirements based on job/task assessments and participation via surveys and interviews of industry practitioners. Consumers of digital forensic results were not included within the scope of this research.

The overall goal was to improve the quality and reliability of digital evidence, to enhance the quality of digital forensics investigations, and to provide a means to determine capability maturity. The proposed model will be based on international standards and best practices, a defined code of conduct, and legal and ethical requirements as a best practice framework, based on detailed research and analysis of what has been attempted so far in the leading countries in this field.

### 1.4.2 Research Questions

In order to achieve the research objective, the following main seven research questions needed to be answered:

1- Does the current system of accreditation of digital forensic labs fully address all the requirements of digital forensics as a scientific discipline, and are these accreditation requirements suitable to digital forensics?

   a. Are they practical and therefore sustainable?
   b. Do they contribute towards the overall improvement of the lab processes and help organisations to achieve operational efficiency and measure capability maturity?
   c. Beyond accreditation, does the present standard governing body offer value (return on investment) to the participating digital forensics labs, and a more effective way to pool collective knowledge and best practices from participating labs and practitioners?
   d. What gaps exist within the current standards used, and what are the key strengths? How can these strengths be utilised in any emerging standard or comprehensive model?
   e. Are the main digital forensic sub-disciplines such as mobile forensics, digital video forensics, and digital audio forensics adequately addressed within the standard? If not, how could these be addressed?
   f. What areas (People, Processes, and Tools) are not being adequately addressed within the prevailing standard?

2. What business drivers and challenges are increasingly affecting accredited labs in the goals to address the standard's requirements, whilst still being pressured with finding a most effective way to address the organisations' business drivers and constraints?
3. Is capability maturity an overlooked means of obtaining operational efficiency within digital forensics, and is it currently being addressed?

4. By consensus, what would digital forensic practitioners and lab managers of new and established labs want to help them to improve their efficiency, knowledge, and budget utilisation?
5. Are the current skills assessment, career development, and progression plans adequately defined within accredited labs? Are organisations able to effectively plan and measure their return on training investments?
6. Would better planning for forensic services and incident response allow for faster gains for organisations if they had the foresight and knowledge of the main services and their prerequisite requirements? Would this enable labs not currently accredited to be able to gain accreditation sooner and at a lower cost?
7. Can this new alternative model cater to both existing and newly founded digital forensics labs?

### 1.4.3 Research Steps

The key research phases as defined within DSRP were expanded upon to produce a more concise sequence of steps applied during the research as listed below:

1. An initial problem definition and identification.
2. Defining objectives of the research.
3. Research existing standards, models, and best practices generally used in Digital Forensic Laboratories.
4. Research requirements for accreditation under ISO 17025/ASCLD-LAB and perceive the challenges of attaining and maintaining accreditation.
5. Designing initial DF-C$^2$M$^2$ tools, methods, processes and project plan for assessments and research.
6. Conduct interviews, assessments and consultations with participating digital forensic practitioners, managers, and investigators.
7. Analyse feedback and findings.
8. Perform Current State Assessment, and SWOT analysis of current offerings, benefits and challenges.
9. Design DF-C$^2$M$^2$, revised assessment tools, workflows, knowledge base goals and criteria.
10. Conduct workshops and seminar on draft DF-C$^2$M$^2$ for review, and solicit feedback and areas for improvement from interviewees.

11. Conduct an audit/assessment of an existing ISO 17025 digital forensic accredited lab against DF-C$^2$M$^2$ requirements. Discuss and review findings with participating lab.
12. Plan and implement updates to the accredited lab to bring it in-line with DF-C$^2$M$^2$ requirements.
13. Solicit feedback from participating lab.
14. Incorporate changes/updates as may be required into DF-C$^2$M$^2$.

At each stage of this research, an effort was made to address the initial research questions stated previously. At each stage of the analysis and solution design process for each of the three key domains, the following questions were posed:

1. What are the present requirements and constraints?
2. What are the present difficulties and challenges affecting each element?
3. How can these challenges best be solved or more effectively managed?
4. How can Capability Maturity be integrated into each element? If so how?
5. Is the proposed solution practical, and cost-effective? If not, how can it made more practical and cost effective e.g.: By including a shared knowledge base to help with ISO 17025 compliant standard operating procedures, and by group testing to tools to address validation requirements, etc.

## 1.5 OUTLINE OF THE THESIS

**Chapter 1:** Introduction to the research, and objectives. It provides a brief summary of the digital forensics environment and highlights the motivating factors behind this research. The contribution this thesis intends to make to the field is stated, and the methodology that will be employed and the limitations of this research are presented.

**Chapter 2:** Will provide a literature review used for this research, including interviews and questionnaires used. It will cover a review of applicable standards in existence, gaps within present standards, integrating multiple related standards into a cohesive system, and a detailed review of ISO 17205 as applied to digital forensics labs will be presented.

**Chapter 3:** Will provide details on the role of practitioners during this survey. It will cover the methods practitioners were engaged, the level of detail, basic demographics, participants labs, and introduced the lab assessments conducted.

**Chapter 4:** Will provide information on the participatory design elements of this research and key stages where participatory design was used as a means to solicit input, feedback and suggested improvements and into which stages this feedback was later incorporated to within this research.

**Chapter 5**: Will define the assessment tools, methods, and criteria used for this research. It will examine the criteria used to evaluate the present standards, based on the research questions defined in Section 1.4.2. The key components and objectives of the DF-C$^{2}$M$^{2}$ will be defined with an analysis of the advantages and drawbacks.

**Chapter 6:** This chapter, addressing design and development, will describe the processes used for the design of the DF-C$^{2}$M$^{2}$ and justifications for the inclusion and the addition of key elements. It will look at each section/module within the DF-C$^{2}$M$^{2}$ and describe how each module fits into the overall DF-C$^{2}$M$^{2}$ framework, and the various design and review stages.

**Chapter 7:** DF-C$^{2}$M$^{2}$ Assessment and Evaluation of DF-C$^{2}$M$^{2}$: will provide details on the DF-C$^{2}$M$^{2}$ assessment of an ISO 17025 accredited lab, the findings, and how this provided confirmation of the need of such a model based on assessment results and participant feedback DF-C$^{2}$M$^{2}$ modularity expansion; this serves as a proof of concept.

This chapter will demonstrate how the DF-C$^2$M$^2$ was updated to include the requirements for cybercrime investigation units, using the same core principles and methods defined in the earlier version of the DF-C$^2$M$^2$, and how ISO 27037 requirements could easily be incorporated, thus providing a demonstration of the expandability of the model, and how interrelated units such as digital forensics and cybercrime investigation can both benefit from shared standards and best practices within the DF-C$^2$M$^2$ framework.

The DF-C$^2$M$^2$ evaluation section will define the participating practitioners and labs, their involvement, methods of review, assessment, and discussions, and feedback and suggestions on improvement of the DF-C$^2$M$^2$.

**Chapter 8:** Conclusion: This chapter will highlight the pros and cons of the proposed DF-C$^2$M$^2$, its limitations, and how these could be addressed. It will also look at the viability of implementing the model on a national scale within a given country, based on workshops with key stakeholders and regulators within that sample country.

## 1.6 SUMMARY

In this chapter, the justification for this research has been set out, and background information in relation to the research problem has been defined, with the key research objectives and questions being stated. The methodology and the novel aspects of the DF-C$^2$M$^2$ model have been defined. The proposed DF-C$^2$M$^2$ has been introduced, including the rationale behind the development of such a model. Some insight is provided into the challenges faced by organisations considering certification vs. accreditation, and some insight about how the model can be applied at an organisational or national scale is presented, as well as what key benefits can be derived from implementing the DF-C$^2$M$^2$.

# CHAPTER 2: LITERATURE REVIEW

## 2.0 INTRODUCTION

This chapter provides a necessary background and review of existing process models related to digital forensics. It provides a current state assessment of present models against the background of the present state of the art, and a review of existing challenges or 'knowledge of the state of the problem' areas as defined within the primary research methodology used.

This chapter presents a literature review of key elements that relate to the People, Processes, and Tools aspects of the proposed new digital forensics model. This chapter will present and discuss the quality management versus capability maturity requirements of typical labs, and the role of ISO 17025. It will present and assess current digital forensics standards, best practices, models, and frameworks versus the present and envisaged future challenges that a majority of digital forensic labs would face. It assesses the completeness of each model, and how they address the People, Processes, and Tools aspects of an organisation.

## 2.1 DIGITAL FORENSIC STANDARDS & BEST PRACTISES

### 2.1.1 Digital Evidence & Forensics Best Practices Background

Digital evidence or electronic evidence may be defined as 'any probative information stored or transmitted in digital form that a party to a court case may use at trial' (Casey, Eoghan, 2004). Digital evidence encompasses any and all digital data that can establish that a crime has been committed or can provide a link between a crime and its victim or a crime and its perpetrator (Kozushko, 2003).

The most prevalent or most frequently referenced guides on digital evidence handling to date have been the Association of Chief Police Officers (APCO)'s Good Practice Guide for Computer-Based Electronic Evidence (APCO, 2013), and the Forensic Examination of Digital Evidence: A Guide for Law Enforcement (NIST, 2004). Both guides are essentially based on the principle that computer-based electronic evidence is subject to the same rules and laws that apply to documentary evidence, within the United Kingdom legal (Common Law) system this is also known as the Best Evidence (Omychund v Barker , 1745) rule, a common law rule of evidence that can be traced back at least as far as the 18th century. In Omychund v Barker (1745) 1 Atk, 21, 49, 26 ER 15, 33, Lord Harwicke stated that no evidence was admissible unless it was 'the best that the nature of the case will allow'. Within the United States, many courts apply the Federal Rules of Evidence to digital evidence (Committee on the Judiciary House of Representatives, 2010).

The following key aspects were examined and evaluated as part of this literature review:

### 2.1.2 Handling and Preserving Digital Evidence: Standards and Guidelines

The first concerted efforts to create a set of (de facto) standard or best practices for the handling and seizure of the history of digital evidence handling can be traced back to the FBI's early initiatives in 1984 (Noblett, Pollitt, & Presley, 2000) . Principles for digital evidence handling are critical elements of the digital forensics evidence process and need to extend beyond implementation and adherence to these best practices within the digital forensics lab, but also to all crime scene units, investigators, incident response teams, and even to corporate organisations. To date, numerous best practices, guides, and standards such as ISO 27037 exist to address these requirements. While several digital forensics models and frameworks address these core requirements, few, if any, cover more advanced subjects that relate to digital evidence examination, analysis, and interpretation of results. It is noted that ISO 27037, 27040, and 27041 were recently released in June 2015, and were not part of the original literature review.

The rapidly evolving nature and sources of digital evidence require that new methods and models be developed to help address the acquisition, preservation, processing, and analysis of such evidence (US Patent No. 2006/0069540 A1, 2006). Challenges and the need to overcome them have spurred innovation and the development of a more scientific approach to digital forensics.

In A Brief History of the FBI (FBI, n.d.) the FBI stated that "In 1984, (tasked with expanded mandate) the FBI established the Computer Analysis and Response Team (CART) to retrieve evidence from computers (it became a full program in 1991)." It also goes on to state that: "The FBI has also played a crucial role in the investigation and prevention of computer crimes. In 1991, the FBI's Computer Analysis and Response Teams (CART) began to provide investigators with the technical expertise necessary to obtain evidence from the computers of suspects". This 'internal standard' later became the foundation of the FBI Computer Analysis and Response Team (CART), and CART training program, handbooks and guides. In order to further develop standards for computer forensic science, the FBI convened a number of international conferences with other law enforcement-related entities in Baltimore in 1995, and in Australia in 1996, and then again in the Netherlands in 1997. The result of these conferences was the establishment of the Scientific Working Group on Digital Evidence (SWGDE) by the Federal Crime Laboratory Directors in 1998 to address computer forensics issues and standards (Pollitt, 2003). In 2002, this development was followed by Request for Comment (RFC) 3227, being categorised as a proposed Best Current Practices (BCP) for Digital Evidence and titled: Guidelines for Evidence Collection and Archiving, was released (Brezinski, 2002).

The SWGDE was formed in response to the increasing digital (versus analogue) evidence sources, and the need to help define best practices for handling and processing this new category of evidence (Pollitt, 2003). The origins of first attempts at helping to define digital forensics as a discipline can be attributed to the early efforts by the SWGDE.

To help illustrate some of the complexity that digital forensic labs face, it is interesting to note that until 2002, the SWGDE and the FBI continued to draft and create best practices or guides on digital evidence handling and processing. To date, the SWGDE has released over 34 best practices and guidelines on subjects related to digital evidence and forensics (SWGDE, 2014).

The Request for Comment (RFC) 3227, categorised as a proposed Best Current Practices (BCP) entitled Guidelines for Evidence Collection and Archiving, was released (Brezinski, 2002). Essentially, the SWGDE, RFC 3227, and FBI's CART programme (FBI, n.d.) all essentially set the basis for digital evidence handling and seizure, and cover topics such as guiding principles during evidence collection, order of volatility, legal and privacy issues, collection steps, and preserving chain of custody.

Until recently, in the absence of any international standards governing the specific handling and preservation of digital evidence, the commonly accepted best practices used and referenced in relation to digital evidence handling have been based on the National Institute of Justice's (NIJ) Forensic Examination of Digital Evidence, a guide for law enforcement used mainly within the United States (NIJ, 2004), and the Association of Chief Police Officers (APCO)'s Good Practice Guide for Computer-

Based Electronic Evidence used primarily in the United Kingdom and some commonwealth countries (APCO, 2012).

### 2.1.3 APCO Good Practice Guide

The APCO Good Practice Guide states that the guide is aimed at:

1. Digital crime scene first responders.
2. Providing guidelines for identification, secure acquisition, preservation, and transportation of digital evidence.
3. Investigators of both high-tech crimes, and crimes where potential digital evidence may be of probative value.
4. Digital evidence recovery staff.
5. External consulting witnesses.

The primary principles as stated in the APCO guide are:

1. ‘No action taken should change data held on a computer or storage media, which may later be required or relied upon in court’ (APCO, 2012).
2. APCO allows some room for situations where changes to data may likely occur as part of the examination process such as when accessing live data rather than a forensic image of that data. The person performing those tasks must be competent to do so, and be able to explain the reasons, relevance, and any implications related to their actions.
3. APCO requires well-documented contemporaneous notes by requiring that an audit trail of all processes executed be created to enable a third party to repeat these steps. ‘An audit trail or other record of all processes applied to computer-based electronic evidence should be created and preserved. An independent third party should be able to repeat those (documented) steps and achieve the same result’.
4. The investigating officer or person in charge is required to ensure that relevant law and the APCO principles are applied at all times.

The APCO sets a good foundation to assist with the correct handling and preservation of digital evidence, but issued as a set of voluntary guidelines for law enforcement officers to follow, and major criticism of the guidelines is that they are not legally mandated as a requirement and individual law enforcement departments are free to choose whether or not to follow these guidelines.

### 2.1.4 The NIJ Guide

The NIJ Guide was designed to provide primarily government agencies and departments with best practices when dealing with and handling digital evidence, and to cover the entire investigation process, i.e. not just digital evidence handling and seizure (NIJ, 2012).

In the absence of any established international standards related to digital evidence handling, the NIJ and APCO guides have been used in many law enforcement and non-law enforcement digital evidence handling teams and digital evidence examination laboratories, with some teams implementing an amalgamation of both guidelines to address areas overlooked in one guide or the other. Whilst the digital forensic community embraced both as accepted best practices, others created other models such as an Advanced Data Acquisition Model (ADAM) (Adams R. B., 2012) related to digital evidence handling that addresses imbalances found in either one or both of the two best practices.

Regarding the fundamental principles as stated within the NIJ guide when dealing with digital evidence, the following general forensic and procedural principles should be applied:

1. No actions taken should affect the integrity of the evidence.
2. Personnel handling and examining digital evidence should have been trained specifically for that purpose.
3. All actions and activities related to digital evidence seizure, handling, and examination should be well-documented and made available for review, if required.

### 2.1.5 ADAM Principles

ADAM’s key principles build upon the ACPO principles and stress the following overarching principles to be followed by digital forensic practitioners (Adams R. B., 2012):

1. Wherever possible, the original evidence should remain unchanged. If the nature of the examination does not allow for this, then the examiners should fully understand and be able to identify the effect that their actions (or the action of their tools) will have on the original data. These changes should be clearly identified and documented in all instances.
2. Detailed records (contemporaneous notes) of all activities from initial acquisition through analysis and reporting should be maintained by all parties involved in the digital investigation process life cycle.
3. Digital forensics practitioners, investigators, and handlers should be competent to perform the tasks assigned to them, and should not attempt to perform any tasks that are beyond their proven competencies and abilities.
4. Legal implications and rights of affected parties should be considered at all stages of the digital investigation life cycle in accordance with prevailing laws and codes of conduct such as EU Data Protection and Privacy laws.
5. Tasks performed on digital evidence should be in accordance with organisational policies and procedures.
6. Maintaining effective communication and associated records is considered to be vital in any digital forensic investigation.

### 2.1.6 APCO, NIJ, and ADAM Limitations

Of the available digital forensics models and best practises reviewed – related to digital forensics evidence handling; neither APCO, NIJ nor ADAM provide a means for assessing and therefore addressing related organisational elements related to People, Process, and Tools requirements. Likewise, by failing to address other organisational domains such as People, Process and Tools; neither enables an incumbent digital forensic laboratory to achieve nor measure capability maturity or performance management.

While these guides help to establish a best practice for digital evidence handling, they only partially address some of the processes that a digital forensic lab may be tasked with and do not address any of the People or Tools aspects of digital forensics. They do not enable or allow an organisation to measure or implement capability maturity across all elements of the digital forensic laboratory operations including digital evidence handling and seizure.

Emerging and recently released ISO standards related to Digital Forensics evidence handling, analysis and processing are reviewed in the sections that follow.

### 2.1.7 ISO/IEC 27037:2012 - Guidelines for Identification, Collection, Acquisition, and Preservation of Digital Evidence

In October 2012, the International Standards Organisation (ISO) published the first standard related to digital evidence handling and preservation titled ISO/IEC 27037:2012 Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence. Four and half years after it was first proposed at a meeting in Kyoto, ISO 27037 is the first internationally accepted, auditable and verifiable standard design to replace existing APCO and NIJ Best Practices (International Standards Organisation (ISO), 2012). These standards seek to address the lack of standards related to digital evidence handling as it relates to the ISO 27001 Information Security series of standards.

The primary goal of ISO 27037 is to help ensure that personnel responsible for handling and acquiring digital evidence do so in a systematic manner that is consistent and legally acceptable (internationally), and is geared towards preservation and integrity of the digital evidence (International Standards Organisation (ISO), 2012).

This international standard also provides general guidelines for the collection of non-digital evidence that may be helpful in the analysis stage of the potential digital evidence. ISO 27037 may also serve to:

- Help decision-makers to decide on the reliability of digital evidence presented before them.
- Guide policy-making bodies that design or assess procedures related to digital evidence handling.

### 2.1.8 ISO 27041 Guidance on Assuring Suitability and Adequacy of Investigative Methods

Although only very recently released on the 15th June 2015, ISO 27041 was reviewed during the final preparation stages of this thesis, and the findings are summarised below.

This standard focuses on the suitability and adequacy of incident response investigative methods. It essentially provides a means for assisting an incident response team in assuring that the processes and tools used in incident response investigations (and subsequent examinations) are ‘fit for purpose’ and can be demonstrated as such.

It stresses the need for verification of tools and methods (as required under ISO 17025) but does not address the additional burden that the need for verification of tools and methods has on lab costs and personnel – often cited as major hindrances for digital forensic practitioners.

### 2.1.9 ISO 27042 Guidance on the Analysis and Interpretation of Digital Evidence

ISO 27042 focuses on the suitability of tools and processes related to the analysis and interpretation of results of digital evidence. Its key areas of focus relate to continuity of the chain of custody via reference to ISO 27037, validity of tools and processes via reference to ISO 27041, and traditional forensic science requirements such as reproducibility of results and repeatability. It is designed to enable independent auditability of processes, results, and findings, and incorporates elements from ISO17025 related to demonstrating the competency and proficiency of personnel.

ISO 27042 emphasises the need for a structured approach to digital forensic investigations. The standard provides guidelines for static and live analysis and draws from ISO 17025 requirements for the competency and proficiency testing of personnel.

### 2.1.10 ISO 27037, 27041, and 27042 Summary of Limitations

1. ISO 27037 does not sufficiently address organisational forensic readiness other than reference to having available tools. Adequate forensic readiness can significantly support the identification, collection, acquisition, and preservation process of digital evidence.

2. ISO 27037 does not provide sufficient guidelines nor requirements regarding the preservation and validation of online evidence for the acquisition and preservation of digital evidence from online sources such as social media. Likewise, it does not cater for evidence that may be provided by a third party such as a social networking service provider (via court issued subpoena), and does not address how the evidential integrity of such data should be validated and preserved.

3. ISO 27037 refers to suggested competency criteria for personnel, but no requirement for proficiency testing of personnel is specified; this should be required by such a standard given the importance of correct digital evidence identification, collection, and preservation procedures as required by the courts as witnessed in the cross-examination of digital forensics expert witness John Bradley (State of Florida v. Casey Marie Anthony , 2008).

4. ISO 27037 refers to the requirements for analysis of log files, etc. but provides no additional guidelines and requirements, and does not refer to related ISO standards specifically, such as ISO 27041 (Guidance on Assuring Suitability and Adequacy of incident investigative methods), ISO 27042 (Guidance on the Analysis and Interpretation of Digital Evidence).

5. ISO 27037 does not provide any guidance nor mapping on how to integrate ISO 27037 with existing laboratory standards such as ISO 17025, when arguably the bulk of teams, i.e. intended end-users implementing ISO 27037, would be part of or work closely with ISO 17025 accredited digital forensic laboratories.

6. ISO 27037, although a welcome addition to digital forensic laboratories policies and procedures, does not address the organisational People, Processes, and Tools requirements. It would enable an organisation to achieve ISO 27037 accreditation, but does not allow an organisation to measure or implement capability maturity across all elements of the digital forensic laboratory operations. The key advantage of ISO 27037 is that the standard has been published, which means that it has been accepted by over 160 nations, and that it provides a globally accepted auditable standard.

7. Both ISO 27041 and ISO 27042 standards are primarily aimed at internal incident response investigations (within an organisation), and as such make certain assumptions about the involvement of the digital forensic/examination team with the incident response team. In most digital forensic laboratories, the investigators, crime scene handlers, and digital forensic examiners reside in separate teams and are governed by separate rules, processes, and requirements.

## 2.2 REVIEW OF DIGITAL FORENSIC MODELS

To determine if any existing digital forensic model or frameworks address capability maturity, and in order to identify any gaps in such model as they relate to the key People, Processes, and Tools elements of a digital forensics laboratory, a review of several digital forensic models and frameworks was performed.

When reviewing existing digital forensic models and digital forensic investigation frameworks, analysis of how they address the People, Processes, and Tools requirements of a digital forensic lab is crucial in helping to identify any gaps, and to determine if they would lend themselves easily to apply capability maturity measurement.

Essentially, digital forensics is a science and a process that can be modelled and structured with some reasonably established phases (Digital Forensic Research Workshop, 2001). In the paper An Approach for Managing Knowledge in Digital Forensics Examinations (Dampier, 2010), the author argued that the majority of digital forensic models and frameworks have focussed primarily on very specific processes, phases, or aspects of an investigation, such as complexity.

Within the past decade, several digital forensic investigation models were identified in a paper titled Systematic Digital Forensic Investigation Model (Agarwal, Saurabh, & Gupta, 2011). Many of these models have been designed and proposed; these include:

- Kruse and Heiser Model (Heiser, 2002)
- Department of Justice (US-DOJ) - Forensic Process Model (Justice U. D., 2004)
- Casey's (Yale) Model  (Casey E. , Digital Evidence and Computer Crime, 2004)
- DFRWS framework meta-model (DFRW, 2001)
- Computer Forensics Capability Maturity Model (CF-CMM)
- Digital Investigation Capability Maturity Model (DI-CMM)

Each model defined a number of unique steps or stages related to digital evidence handling, examination, and storage. Some extended their model to cover elements of investigation, planning, review, and reporting, but none extended their models to examine issues related to capability maturity, efficiency, integration with international standards, or quality management processes. Essentially, the vast majority of the models tend to focus on addressing some aspect of the ‘Process’ component of the proposed digital forensics model.

### 2.2.1 Kruse and Heiser

Kruse and Heiser in the Lucent/Kruse Heiser Model state that computer and network forensics methodologies consist of three basic components, sometimes referred to as the ‘three A’s’ of computer forensics investigations.

The three A’s are:

1. Acquiring the evidence while ensuring that the integrity is preserved. This involves:
    a. Establishing and maintaining a chain of custody
    b. Collection
    c. Identification
    d. Storage
    e. Documentation (of the investigation and examination processes)
2. Authenticating the validity of the extracted data (ensuring that it is the same as the original)
3. Analysing the data whilst preserving its integrity.

In this model, the authors state that complete and detailed documentation should be made at each step of the investigation, and make provisions within their proposed model to cater to an event that may result in the forensic integrity or authenticity being affected, by stating that documentation or contemporaneous notes are vitally important in instances where the authenticity of the digital evidence was not preserved.

**Limitations:**

The Kruse and Heiser model is process-centric, identifying steps and distinct stages in a digital forensic examination, and key emphasis is placed on documentation and authenticity. It does not address issues and requirements related to People, Tools, Quality Management, and Capability Maturity.

### 2.2.2 The US-DOJ (Forensic Process Model)

The U.S. Department of Justice published a process model designed for use in electronic crime scene investigation. Aimed at digital evidence first responders (DEFRs), the guide consisted of four phases:

A. **Collection:** This involves the evidence search, evidence recognition, evidence collection, and documentation.

B. **Examination:** This is designed to facilitate the visibility of evidence, while explaining its origin and significance. It involves revealing hidden and obscured information and the relevant documentation.

C. **Analysis**: This looks at the product of the examination for its significance and probative value in the case.

D. **Reporting**: This entails writing a report outlining the examination process and pertinent data recovered from the overall investigation.

**Limitations:**

The US-DOJ model is more process-centric, identifying the DOJ's proposed steps in a four-stage digital forensic examination process. The DOJ model does not attempt to address any underlying issues or additional requirements that could affect the overall quality and capability of both the model and any processes derived from this model.

Key areas overlooked by the DOJ model are those that relate to requirements for control and processes for assuring the quality of People, the various Tools and methods used, the need for an all-encompassing Quality Management approach to digital forensics, and the need for being able to measure Capability and Process Maturity.

### 2.2.3 Casey (Yale) Model

A security administrator at Yale University, Eoghan Casey designed a model known as Casey's Digital Evidence Guidelines that focussed on the processing and examination of digital evidence. The Casey model categorised the stages into six distinct steps:

- **A.** Preliminary Considerations
- **B.** Planning
- **C.** Recognition
- **D.** Preservation, Collection, and Documentation
- **E.** Classification, Comparison, and Individualisation
- **F.** Reconstruction

**Limitations:**

The Casey (Yale) Model is process-centric. It helps to identify steps and distinct stages in a digital forensic examination from planning, evidence identification and acquisition, classification, validation (of results), and reporting. The Casey model omits underlying requirements related to skills (people), additional supporting business and quality processes, process/performance measurement, and personnel efficiency.

### 2.2.4 Digital Forensic Research Workshop (DFRW -2001)

The Digital Forensic Research Workshop (DFRW) created a consensus document that outlined the state of digital forensics at that time. During this meeting, the participants agreed by consensus that digital forensics was an essentially a scientific process and they attempted to document the various elements within that process in what is known as the DFRW Model – 2001. The key steps within this model are:

1. Identification
2. Preservation
3. Collection
4. Examination
5. Analysis
6. Presentation
7. Decision

The steps listed above were designed to cover both the technical and non-technical requirements of the digital forensic examination process.

**Limitations:**

Although more detailed than the previously reviewed models, the DFRW is still very task-specific/process-centric in its approach. Due to its more detailed stages, and due to the fact that it was one of the very first attempts at defining a process model for digital forensics, the DFRW has been widely adopted as the basis for many derivative models and approaches.

DFRW provides a more granular view of the digital forensic examination process requirements, but fails to address other elements that could adversely affect the efficiency of the model such as People (Skills, Competency and Proficiency, and Efficiency), Tools and Methods, and overall Capability Maturity.

### 2.2.5 Computer Forensics Capability Maturity Model (CF-CMM)

The Computer Forensics-Capability Maturity Model (CF-CMM) is a patent (US Patent No. 2006/0069540 A1, 2006) (abandoned in 2008). CF-CMM is described as a '… method for assessing capability and maturity of an organization's computer forensics processes. It defines an architecture for a computer forensics capability and maturity model (CMM), a computer forensics CMM appraisal method, implements the computer forensics CMM for improving computer forensics processes within the organization, and conducts an appraisal of the organization according to the CMM appraisal method' (US Patent No. 2006/0069540 A1, 2006).

The CF-CMM presents a method to categorise processes used internally within an organisation by examining their forensic architecture and processes. It is designed as an assessment method for use within internal organisations that provide forensic services to internal customers and systems, and could be considered to be part of an organisation's internal computer forensics readiness assessment.

Key steps and areas covered as defined with the CF-CMM are categorised within two groups of processes:

- Group One processes includes ten steps that draw a parallel to the seven steps essentially covered in the DFRW model from the identification of electronic devices as potential sources of evidential (investigative) value through documenting and securing the crime scene, transportation and preservation of evidence, and conducting of the forensic examination, generating the report, and presenting the findings.
- Group Two processes cover two process areas including ensuring quality, and providing ongoing skills and knowledge.

The CF-CMM presents a methodology for applying CMM to generic computer forensic processes and to conduct a Computer Forensics CMM Assessment (CFAM).

The CF-CMM specifies five levels of maturity:

- Level 1 - Informally performed processes,
- Level 2 - Planned and tracked processes,
- Level 3 - Well-defined processes,
- Level 4 - Quantitatively controlled processes,
- Level 5- Continuously improving processes.

**Limitations:**

The CF-CMM was published as a patent owned, designed, and created by its author based on his views and understanding of the specific requirements for computer forensics in 2004. The patent application was subsequently abandoned in 2008. 'The basic philosophy behind Computer Forensics CMM is to empower computer forensics-related organisations to develop and improve a process that is most effective for them'. (US Patent No. 2006/0069540 A1, 2006), as opposed to international standards, or benchmarks.

Not all organisations are able to effectively define and standardise their processes – this is especially true of new organisations that may lack the prerequisite experience to do this effectively, and therefore may need the ability to draw from a knowledge base of processes, tools, and guidance as defined within the proposed digital forensics model. Kerrigan stated that the CF-CMM as a CMM for digital investigations is incomplete as it focusses on the computer forensics aspects of the investigation (Kerrigan, 2013). Likewise, the CF-CMM is incomplete with regards to digital forensics, as it does not cater to the changing needs of digital forensics, which have since evolved from traditional computer forensics.

The CF-CMM also fails to address the need for conformance with international best practices and standards such as ISO 17025, and it does not address the key organisational elements – People, Processes, and Tools.

The CF-CMM’s key elements are not based on a broader consultative approach – sourcing input from accredited labs and practitioners, thus potentially limiting the scope, sphere of influence, practicality, and acceptability within the digital forensics community. Designing processes that are the most effective for them is important, as an organisation has now been superseded by the need to design processes that meet the current challenging legal standards and technology requirements.

Additionally, while the CF-CMM looks at ‘providing access to investigative tools and equipment’ (US Patent No. 2006/0069540 A1, 2006) in its Group One processes, it does not address the legal and accreditation needs for well-established processes for the validation and testing of tools and methods to be used for digital forensic examinations.

The CF-CMM uses CFAM as its assessment method, which is neither aligned nor compliant with the requirements of ISO 17025 or the ASCLD-LAB supplemental requirements, nor does it facilitate integration with new, emerging related ISO standards such as ISO 27037, ISO 27041, etc.

The CF-CMM does not adequately address key aspects of digital forensics such as people, tools, and compliance, or integration with standards and regulatory requirements.

### 2.2.6 Digital Investigations Capability Maturity Model (DI-CMM)

The Digital Investigations Capability Maturity Model (DI-CMM) (Kerrigan, 2013) focusses on five generic groupings of tasks associated with digital investigations, namely Pre-process, Acquisition and Preservation, Analysis, Presentation, and Post-process. The DI-CMM focusses on three organisational elements – People, Process, and Technology.

The DI-CMM focusses on the broader subject of digital investigations from start (Pre-process) to completion (Post-process), an element of which (Analysis) may include examination of digital forensic artefacts and draws heavily from the Extended Model of Cybercrime Investigation (EMCI) (Ciardhuain, 2004) in all process areas. The DI-CMM identifies 15 key stages of a digital investigation, and provides a basis for assessing capability maturity in each of those 15 areas, including Digital Forensics or Storage, Examination, and (perhaps) Presentation, which relate directly to digital forensics lab processes. The other 12 stages are more specific to investigative teams that often work independently of the digital forensic laboratories in most law enforcement organisations.

While the DI-CMM provides a sound foundation for applying CMM to digital investigations, its core focus is within the scope of an investigator and it provides little detail about the requirements for implementing CMM within the scope of digital forensics.

However, the DI-CMM is not geared towards focussing exclusively on the specialist area of digital forensics or digital forensic labs, nor does it address the requirements of digital forensics labs and examinations in any significant detail – it is a model aimed at digital investigations and focusses on the various stages of an investigation. Digital forensics-specific elements account for only a small part of the model in its entirety, and digital forensics is not adequately covered in sufficient detail to enable an organisation to achieve CMM level 5 maturity, nor does it enable an organisation to truly understand its required processes and how best to optimise them.

Although the DI-CMM includes general overviews of three key elements – People, Processes, and Tools – it does not address the Capability Maturity requirements of each, nor does it provide any tools to measure and address any areas of deficiency within the organisation, or provide recommended approaches or plans for addressing any deficiencies.

The DI-CMM is neither aligned nor compliant with the requirements of ISO 17025 and ASCLD-LAB supplemental requirements for digital forensic labs.

The DI-CMM does not adequately address key aspects of digital forensics such as People, Tools, and Compliance and Integration with standards and regulatory requirements.

### 2.2.7 Common Limitations of Digital Forensic Models

Of all of the models reviewed, none of the above digital forensic models addressed the three key organisational elements that affect the quality of digital forensics, namely People, Processes, and Tools. The DI-CMM is perhaps the exception, but it is focused on digital investigations, of which only a small section covers digital forensics and the People, Process, and Tool components are covered only briefly.

## 2.3 ISO 17025 - UNDERSTANDING THE ORGANISATION, QUALITY, AND ISO 17025 RELATIONSHIP

The ISO/IEC 17025 standard relates to the general requirements for the competence of testing and calibration laboratories. This standard, although specific to testing and calibration laboratories, is essentially an extension of the ISO 9001 Quality Management standard.

ISO 17025: 2005 and the US equivalent (ASCLD/LAB) requirements (including the ASCLD-Lab supplemental requirements International Accreditation for Forensic Science Testing Laboratories) were reviewed as part of this research.

ISO 17025 is a general standard that can be applied to a wide variety of testing (and calibration) laboratories such as forensic, environmental, pharmaceutical, food, material testing, health service laboratories, and in the absence of a better alternative, more recently the standard has been applied to digital forensic laboratories and processes.

The ISO 17025 requires laboratories to address issues that directly affect data quality (results) and technical competence of personnel. The standard's goal is to ensure that quality principles are consistently applied, and that any deviations from these defining principles are well-documented, controlled, and restricted. ISO 17025 is seen as a means of assurance that scientific principles related to laboratory tests and quality management systems are uniformly applied by the accredited laboratory.

Laboratories use ISO/IEC 17025 to implement a quality system aimed at improving their ability to consistently produce valid results. It is also the basis for accreditation from an accreditation body. Since the standard is related to competence, accreditation is simply formal recognition of a demonstration of that competence. A prerequisite for a laboratory to become accredited is to have a documented quality management system. The usual contents of the quality manual follow the outline of the ISO/IEC 17025 standard.

### 2.3.1 ISO 17025 – People: Training, Certification, and Accreditation

The number of professional certifications, results of competency and proficiency tests are often used as a means of quality measurement for personnel with digital forensics laboratories. ISO 17025 requires that personnel performing tasks have been trained, competency tested and those tasks, and that those designate as Digital Forensic Examiners participate in proficiency tests. These indicators whilst useful, fall short in providing any meaningful measurement of quality or capability maturity of personnel.

Within the context of quality management and business improvement processes; “Performance measurement forms an integral part of the management processes and systems within (…) an organization” (Sinclair & Zairi, 1995). “Measurement is the trigger for process improvement and the achievement of superior competitive standards” (Sinclair & Zairi, 1995). It could therefore be argued that effective quality and performance management can only be achieved by applying quality management principles and performance benchmarking across of the three core aspects of an organisation, namely its People, Tools, and Processes.

“Capability Maturity can be applied to various collective processes and elements of systems development, information gathering, and personnel via the People Capability Maturity Model (P-CMM). People Capability Maturity Model (P-CMM) applies the very same assertions proposed by Sinclair and Zairi, and can influence an organisation’s personnel quality management ethos and expectation.

When assessing personnel or the people aspect of an accredited digital forensic laboratory from a quality and capability perspective, several key elements need to be addressed, and these are:

1. Competency and proficiency testing
2. Certification
3. Training (on the job and formal) and career progression paths
4. Accreditation.
5. Capability Maturity and Performance Measurement.

Each of these requirements is discussed in further detail below:

#### 2.3.1.1 Competency and Proficiency Testing Requirements for Digital Forensics Specialists under ISO 17025 and ASCLD-LAB

The need for effective competency and proficiency testing of digital forensic staff is a critical and justified ISO 17025 requirement. However, gaps and disparities within the present competency and testing requirements within ISO 17025 have highlighted the need for a more extensive competency and proficiency testing regime.

**Background:**

Within the scope of the American Society of Crime Laboratory Directors / Laboratory Accreditation Board (ASCLD-LAB) accreditation statement of requirements, both internal competency tests and external proficiency tests of technical staff are required (ASCLD/LAB, 2014). ASCLD-LAB accreditation covers the requirements of ISO 17025 with additional supplement requirements. The requirements for competency and proficiency testing of digital forensic personnel within ISO 17025 are adapted from the ASCLD-LAB requirements, and ASCLD-LAB technical assessors are employed globally to assist with technical assessments of digital forensic lab personnel and technical procedures by the majority of ISO 17025 accreditation bodies.

The ASCLD-LAB standard defines the requirements for proficiency and competency testing of examiners in order for an accredited laboratory to obtain and retain its accreditation. Under the requirements of the ASCLD-LAB (ISO17025:2005) proficiency review program, digital forensic analysts and engineers are required to be proficiency tested in at least one Digital and Multimedia Evidence sub-discipline (e.g. computer forensics, including mobile devices, forensic audio, video analysis, and image analysis) in which they perform a digital forensic examination or analysis services. ASCLD/LAB accreditation requires that laboratories have certified examiners on staff. However, all digital forensics examiners and analysts must undergo an ASCLD accredited lab’s documented and approved certification process, and may not perform examinations independently until they have done so.

The ASCLD-LAB accreditation process requires digital forensics specialists (examiners) to be proficiency and competency tested at set intervals, in order for an ASCLD-LAB accredited digital forensics laboratory to obtain and retain its accreditation. It requires trainee digital forensics specialists (examiners) to be mentored and then tested on both technical and procedural aspects of digital forensics examination, and certified internally within an organisation as competent.

Clearly, proficiency testing is an integral part of both ISO 17025 and ASCLD-LAB's requirements. Proficiency testing can be used as a means to identify weaknesses within the basic skill set that need to be remedied. Ideally, proficiency tests should provide a reliable method of verifying that the minimum required skills and basic processes are in place, and that required digital forensics best practice and ISO 17025 process requirements are being applied. As to whether the present regime of digital forensic proficiency testing requirements adequately address all aspects of a digital forensic examination including quality management, analysis and reporting would need to be investigated further as part of this research.

Proficiency test providers exist for Computer Forensics and Digital Video Forensics (ASCLD/LAB, 2014), but no such providers exist for Mobile Phone Forensics, Digital Audio, or Online Evidence (e.g. Cloud Forensics), to date[2]. As both ASCLD-LAB and ISO 17025 accredited digital forensic labs often provide more than just computer and digital video forensics, but can be accredited for mobile phone forensics, it raises issues about (in reality) how critical such tests are for obtaining and maintain accreditation, in view of the fact that mobile phone forensics, typically account for a significant number of the devices examined of all devices examined in law enforcement laboratories by virtue of the pervasiveness and use of mobile devices for accessing the majority of social networking applications (Adams, Whitledge, & Shenoi, 2008)

The majority of accredited digital forensic labs are accredited for computer and mobile phone forensics, and yet no external proficiency tests exist for this sub-discipline. In such instances, the ASCLD-LAB and ISO 17025 requirements for external proficiency testing of examiners can be replaced with an 'inter-lab comparison' test between two or more digital forensic labs.

[2] Mobile forensics external (paid) proficiency tests became available in 2015.

The requirements for ISO 17025 accredited laboratories performing digital forensic tests (examinations) as defined within the American Association for Laboratory Accreditation (A2LA) R103a – Annex – Proficiency Testing for ISO/IEC 17025 Laboratories document are listed below (A2LA, 2013):

**Digital Forensics:**

- Digital media examination (e.g. Write protection, Media imaging, Establishing a hash value of the original media, Creating a directory listing, Recovery of all active files, Deleted file recovery, Metadata recovery from documents, and Text file recovery),
- Analogue video examination, and
- Digital video examination.

**Competency tests:** Within both ISO 17025 and ASCLD-LAB: a requirement for individual competency testing prior to assuming casework is required for all levels of technical staff responsible for handling or processing digital evidence (ASCLD/LAB, 2012). The major challenge faced by digital forensic laboratories in this regard has been creating and conducting such tests for every aspect of digital forensic processing and examination, and keeping the competency tests relevant and current. Essentially, the goal of the test is to ensure that lab personnel are able to perform specific technical tasks related to digital evidence using the processes and technical procedures defined as part of their ASCLD-Lab/ISO 17025 documentation set.

During the assessment of accredited digital forensic labs and in related interviews, it was noted that the requirements for competency tests merely extended to the most basic tasks, such as USB media imaging, or workstation verification. There were no requirements for such competency tests to extend beyond these basic tasks into areas such as using computer forensic tools, analysis, or data, or interpretation of results. Even during assessments by ISO 17025/ASCLD-LAB technical assessors, the witnessing of competency tests covers only the most basic of tasks (LAB_A, 2013), and no provision within the standards allows for, nor requires, detailed process efficiency and People Capability maturity elements to be included in either the competency or proficiency tests.

Likewise, by focussing primary on the least time-consuming, most basic tasks during the witnessing of competency tests, the most time-consuming aspects of digital forensics examinations -- analysis, interpretation of results, and reporting -- are overlooked and yet, ironically, these are the key technical areas of a digital forensic examination process that need to be evaluated, measured, and optimised via people and capability maturity model guidelines.

Digital forensic examiners may be able to perform the most basic required digital forensic tasks during ISO 17025/ASCLD-LAB technical assessments with ease, and yet fail in adequately conducting detailed analysis of artefacts and interpretation of results. Likewise, the method(s) used to perform analysis tasks may not be efficiently organised or optimised, resulting in specific forensics tasks such as 'data carving' having to be performed more than once or in a less than efficient and timely manner. Based purely on these elementary competency testing requirements, laboratories may be lulled into a false sense of efficiency and competency.

In summary, while the principles behind the need and justifications for competency and proficiency testing within ISO 17025 and ASCLD-LAB are sound, they fail in execution and in the level of detail required. Ideally, proficiency tests should cover not just the elementary tasks, but also analysis, interpretation of results, and reporting.

Additionally, it can be argued that proficiency tests should help to ascertain whether the digital forensics examination lab processes are being performed in the most efficient and cost-effective manner – as essentially, proficiency examinations should test both personnel and lab processes used by those personnel. Enhanced proficiency testing within digital forensics has the potential to also help determine whether the personnel performing these examinations, and the processes and tools applied, have achieved the optimum level of capability maturity.

#### 2.3.1.2 Requirements for Proficiency and Competency Tests

With ASCLD-Lab and ISO 17025, the requirements for external proficiency testing are as follows:

1. **Requirements Under ISO 17025**:
   ISO 17025 and ASCLD/LAB require that an accredited laboratory has a system for managing and monitoring the quality of examinations; and that it conform to scientific principles regarding validity of results, validation of methods and demonstrated competency of personnel (ASCLD/LAB, 2014). This means that laboratories must perform internal performance-based quality control checks in accordance with 5.9 of ISO/IEC 17025 as it applies to every test, technology and/or parameter on their Scope(s) of Accreditation in order to demonstrate compliance with ISO/IEC 17025 accreditation requirements.

Additionally, ISO 17025 requires that in addition to all of the lab's quality controls, independent proficiency testing (PT) of all personnel involved in examinations is required, as and where available, as described in A2LA R103a –Annex– Proficiency Testing for ISO/IEC 17025 Laboratories document (A2LA, 2013) (American Association for Laboratory Accreditation, 2013). This document states that laboratories are required to participate in inter-laboratory comparison tests or commercial proficiency tests twice a year. Additionally, staff involved in any stages of forensic testing or preparation should participate in inter-laboratory comparison and/or external proficiency tests annually (subject to ruling by the lab's accrediting body's requirements).

A major obstacle to achieving and fulfilling these goals from a digital forensic perspective at present is that commercial proficiency tests are currently only available for computer forensics, and more recently digital video forensics. Mobile phone forensics - which account for the majority of all devices examined within most digital forensic labs (Adams, Whitledge, & Shenoi, 2008) has historically had no ASCLD-LAB approved commercial proficiency tests available until 2015 (Dolin, 2015). The alternate route of mobile forensics proficiency testing via inter-lab comparison of results is not a viable solution for many digital forensic labs as, obtaining cooperation with other accredited labs to participate in inter-lab comparative testing is potentially costly, difficult to plan, manage and independently assess.

While some may argue that the presently available digital forensic (external) commercial proficiency test are adequate to cover mobile and computer devices, the differences between how standard digital computer media and mobile devices should be handled, imaged and analysed, and the difference in toolsets and skill sets required for each type of device examination demands that examiners are proficiency tested in each type of examination as the recent introduction of ASCLD-LAB (ISO 17043) approved mobile forensics proficiency tests proves.

2. **Requirements Under ASCLD/LAB:**
   Participate annually in and successfully complete at least one (1) external proficiency test for each forensic discipline in which it provides services and is accredited by ASCLD/LAB. The required external proficiency test(s) must be obtained from an ASCLD/LAB approved proficiency test offered by an ASCLD/LAB approved test provider.

Ensure that *each* analyst completes at least one proficiency test annually in each discipline in which the analyst performs casework examinations. The annual tests taken by analysts may be from internal or external sources (ASCLD/LAB, 2014).

#### 2.3.1.3 People - Certifications: Commercial and Vendor-Specific

Certification implies that an individual has attained a certain Body of Knowledge (a baseline to measure or compare against), and counters the global trend in which an examiner is deemed a ‘specialist’ after attending a course in digital forensics. In general, the primary goal of certification is to provide some form of proof of competency or proficiency in a particular subject; however, from a legal and digital forensics perspective, within digital forensics, in addition to providing a benchmark that attests to the fact that an individual has demonstrated knowledge in a particular area, Krause argues that the main motivation for obtaining certification by digital forensics personnel is to help boost the credibility of the digital forensic examiner before the courts (Krause, 2010).

Commercial, vendor-specific testing and certification on the use of certain digital forensics products such as Encase Certified Examiner (EnCE) (EnCE® Certification Program, n.d.), AccessData Certified Examiner (ACE, n.d.) , and similar products have been available for some time. These certifications and exams are largely focussed on testing the candidate's proficiency and knowledge of the commercial product, and do not test broader aspects (policies, procedures, and principles) of the digital forensics discipline.

While these certifications or credentials listed above add value and a degree of assurance that the holder understands the use of a specific commercial tool, and some basic theory related to digital forensics, they *do not* attest to their broader knowledge of digital forensics. Many would argue that such certifications, although they have a place within the broader set of requirements, attest to the candidate's knowledge of the product, rather than of digital forensics. The view that such certifications allow for the certification of digital forensics 'product specialists' is widely supported amongst the industry, and product certification should be viewed as a baseline test of a candidate's understanding; they do not make the candidate a digital forensics specialist, nor do they attest that the candidate knows everything there is to know about the product.

#### 2.3.1.4 People Certifications: Vendor-neutral

Vendor-neutral training and certification related to digital forensics is also available primarily via two popular training providers, namely SANS Institute (SANS) and EC-Council (EC-Council). The certification offered by each is Certified Hacking Forensics Investigator (CHFI) (EC-Council) from EC-Council, SANS GIAC Certified Forensic Analyst (GCFA), and SANS GIAC Certified Forensic Examiner (GCFE) (GIAC, n.d.). Each of these certifications offers a vendor-neutral approach to the subject and uses a wide variety of forensic tools. These courses tend to be more technical in-depth than the product-oriented certifications and focus on procedures and methodology more than the product certification and training that providers do. By addressing the forensic aspects of technology, as well as fundamentals, they address a gap in a forensic examiner's knowledge, but as commercial certifications they are not as widely accepted within the law enforcement community due to the fact that neither provides and that their syllabus is not recognised or accredited under the ASCLD-LAB (ISO 17025) proficiency testing accreditation.

In summary, certification should be considered as a measurement of a candidate's proven technical ability within a specific scope. Certification is essentially a baseline, and does not make the candidate an expert, but simply states that they have met a minimum baseline (standard) with regards to their understanding, competency, and proficiency of a given subject. Certification can be used as a factor in the overall P-CMM of an examiner or a group of examiners within a digital forensic lab[2], but the P-CMM provides a more holistic view of the candidate's skills, process knowledge, and ability to perform optimally and efficiently under a wider range of circumstances.

#### 2.3.1.5 ISO 17025 Tools – Validation and Testing

Within the scope of ISO 17025, the requirements for the validation of tools and methods are critical as a means to help ensure the quality of results by evaluating the tools and methods to be used for testing. Legal requirements regarding admissibility of evidence, and accepted scientific rules related to Daubert and Frye make the requirements for adequate testing and validation of tools and methods both a legal and a scientific requirement. There is a critical need in the law enforcement community to ensure the reliability of computer forensic tools (NIJ, 2012). Validation of tools and methods is a key requirement, and capability maturity can be applied to validation of methods (processes), as well as the processes used to test and validate tools. Validation of tools and methods was also identified as a critical time-consuming and costly exercise that all accredited labs needed to comply with. Applying elements of the Software Capability Maturity (CMM) to the processes used to validate and test tools and methods and the prospect of being able to pool participant lab resources to reduce the costs of such exercises formed the motivation to research and assesses validation of tools and methods best practices and requirements in more detail.

Within the context of ISO 17025 (Clause 5.4 Examination (Test) Methods and Method Validation) (ISO/IEC: 17025:2005) and digital forensics, digital forensic laboratories will use tools, methods, and procedures that have been adequately tested and validated for examination of digital evidence. Prior to use by digital forensic examiners, any critical equipment, software, and media that can impact the outcome of examinations or results must validate and/or verify performance, as applicable. Tools and methods must be validated to ensure that they are known to function correctly for the intended examination, and have been tested for accuracy and to identify any deficiencies or limitations. Tools such as forensic write blockers, etc. must be calibrated or performance-verified prior to their use in each examination.

The National Institute of Justice (NIJ) Computer Forensics Tool Testing (CFTT) program is the leading vendor and independent provider of validation testing of digital forensic tools (for both mobile phones and computers) (CFTT, 2013).

The goal of the Computer Forensic Tool Testing (CFTT) project at the National Institute of Standards and Technology (NIST) is to establish a methodology for testing computer forensic software tools by the development of general tool specifications, test procedures, test criteria, test sets, and test hardware. The results provide the information necessary for toolmakers to improve tools, for users to make informed choices about acquiring and using computer forensics tools, and for interested parties to understand the tools' capabilities. This capability is required to ensure that forensic software tools consistently produce accurate and objective test results, and the tests conducted by NIJ CFTT are based on internationally established and recognised methods for validation and conformance testing (NIJ, 2012).

The CFTT approach to the validation of tools in order to support the legal requirements related to the validity of results (Daubert) and should be performed in a uniform, well-structured, and internationally recognised manner (NIJ, 2012). Additionally, shortcomings discovered during testing of tools should be disclosed to enable developers to improve their tools, and to allow for users to make informed choices, and for the legal community and others to understand the tools' capabilities (NIJ, 2012). The results are publicly posted and are available for review and feedback from the digital forensics community (NIJ, 2012).

The CFTT methodology is developed by NIST (CFTT, 2013). The methodology is based on functionality such as write-blocking, disk imaging, data carving, and file format decoding etc., and tests are developed for each distinct category or function (CFTT, 2013) . Although digital forensic tool vendors may request testing of their product, the CFTT Steering Committee decides which products to test based on the popularity of the product according to users' requests (CFTT, 2013). More information on the CFTT/NIST specification development process is taken from CFTT and is shown in Appendix H.

#### 2.3.1.5.1 CFTT Limitations

The main concerns regarding CFTT results are that the tools tested are often outdated by the time that test results are published. Digital forensic labs using mobile forensic tools, which are on average updated almost monthly since 2010 (Cellebrite, n.d.), are often left with a dilemma in that, in order to perform a digital forensic examination on a newly released handset (that may be supported by the latest release of their preferred forensic examination tool), the tool version may not have been independently validated or tested by an organisation such as NIST. CFTT test results or products can be version-specific. The lab is faced with the decision of:

1. Either conducting their own validation tests on the newest version of the tool, a task that is time-consuming and requires a sound validation testing process, specifications, and known test data. The process of self-testing the tool may also be disputed in court as not being adequate or sufficient, thereby potentially invalidating any results (digital evidence) obtained using that tool, or
2. Opting not to use the latest version of the tool, and in the process, not being able to successfully examine the handset, or
3. Use the older (tested) version of the tool, but run the risk that the data may not be interpreted correctly.

Next, CFTT does not provide any validation or testing of methods (technical processes). While many rely on guides such as ACPO guide for digital evidence handling, scenarios such as this occur often, and labs are left to improvise and perhaps use untested tools and non-validated methods to obtain, process, and analyse digital forensic evidence. The ability of a lab to demonstrate and assess its ability to perform rigorous and adequate testing of tools and methods is a critical accreditation, legal and regulatory requirements (in most countries) and these requirements can be adequately assessed and addressed via the use of CMM elements applied to tools and methods validation and verification testing processes.

### 2.3.2 Summary of ISO 17025 Limitations

Several limitations regarding ISO 17025 as they related specifically to digital forensic laboratories were discovered via reviews of the standard, assessments, and interviews. Table 2 highlights some of the limitations of ISO 17025 when applied specifically to the discipline of digital forensics:

Table 1: The ISO 17025 limitations

| Standard Addresses | ISO 17025 | ISO 17025 Comment |
|---|---|---|
| Quality Management System | **Addressed** | • Applies to general requirements with a requirement for competency added to it.<br>• Does not address requirement for process and capability maturity.<br>• QMS is largely based on ISO 9000 standard. |
| Competency of Personnel | **Partially Addressed** | • Too broad.<br>• Insufficient level of competency testing required.<br>• General: does not provide specific guidelines/requirements for each technical job role.<br>• Competency testing requirements are usually restricted to low-level complex tasks such as imaging and write block verification. No requirements for analysis and examination of results. |
| External Proficiency Testing/Inter-lab Comparison | **Partially Addressed** | • Based on ISO 17024: Only currently available for Computer and Digital Video sub-disciplines. Not available for Mobile examinations.<br>• Level of tests does not distinguish between the junior versus senior examiners, and is generally less challenging than professional certification exams such as CCE. |
| Health & Safety | **Addressed** | • More in line with dealing with conventional lab testing requirements. |
| Independently Auditable | **Addressed** | • Well-established standard, with hundreds of assessors worldwide. However, fewer than 10 active ASCLD-LAB technical assessors are known to provide technical ISO 17025 assessment of digital forensic labs. |
| Internationally recognised | **Addressed** | • Close to 100 digital forensic labs (ASCLD-LAB and ISO 17025) accredited worldwide. Mainly within law enforcement. |
| Validation of Tools and Methods (*repeatable* and *reproducible)* | **Partially Addressed** | • Stated as a requirement.<br>• Does not take into account the wide number of tools that may be used, or the amount of time and effort required to test each new version of each tool.<br>• Labs are free to define test data set, and test results may not be accurate (no independent verification). |
| Individual Certification/ Licensing Requirement | **Not Addressed** | • Not stated as a requirement. |

| Standard Addresses | ISO 17025 | ISO 17025 Comment |
|---|---|---|
| Digital forensics specific / caters to specialisation(s), e.g. Mobile Forensics, Digital Video Forensics, Network Forensics | **Not Addressed** | • ISO 17025 is a general multi-purpose standard that does not address requirements specific to digital forensics. It is therefore adopted rather than being adapted to digital forensics labs. |
| Provides organised training and career progression paths per technical job role | **Partially Addressed** | • The requirements are that job descriptions define roles and responsibilities and that staff received training and competency testing. |
| Costly to design and implement, SOPS, Audit requirements and Technical SOPs | **Partially Addressed** | • Standard SOPs need to be developed, which is both time- and skills-intensive. |
| Covers Digital Forensics First Response Training, SOPS, and Processes | **Not Addressed** | • Could affect overall evidential integrity. |
| Addresses Information Security of Data | **Not Addressed** | • Confidentiality, integrity, and availability of information that may include digital evidence derivative results are not addressed. |
| Covers Incident/Digital Crime Scene Handling | **Not Addressed** | • Not required/provided, although the integrity of evidence from a holistic perspective requires evidential integrity to be maintained from digital crime scene to the lab (add ISO 27027). |
| Covers Potential Evidence Identification | **Not Addressed** | • Not required/provided |
| Covers Digital Evidence Collection | **Not Addressed** | • Not required/provided (add ISO 27037) |
| Cover Digital Evidence Transportation | **Not Addressed** | • Not required/provided (add ISO 27027) |
| Covers Digital Evidence Storage | **Not Addressed** | • Not required/provided (add ISO 27037) |
| Digital Evidence Acquisition (Capture) | **Not Addressed** | • Not required/provided |
| Digital Evidence Analysis | **Not Addressed** | • Not required/provided |

| Standard Addresses | ISO 17025 | ISO 17025 Comment |
|---|---|---|
| Digital Evidence Interpretation | **Not Addressed** | - Not required/provided |
| Digital Evidence Validation | **Partially Addressed** | - Very broad and general, with no specific guidelines or requirement related to the discipline of digital forensics |
| Preserving Digital Evidence | **Partially Addressed** | - Very broad and general, with no specific guidelines or requirement related to the discipline of digital forensics |
| Case/Investigation Planning | **Not Addressed** | - Not required/provided |
| Information/Workflow Rules | **Not Addressed** | - Not required/provided |
| Digital Forensic Tool and Equipment Validation (Calibration) | **Partially Addressed** | - Very broad and general, with no specific guidelines or requirement related to the discipline of digital forensics. |
| Report Writing | **Partially Addressed** | - Not specifically addressed in any detail. |
| Presentation/Digital Forensics Expert Witness | **Not Addressed** | - Not required/provided |
| Licensing Model for Practitioners | **Not Addressed** | - Not required/provided |
| Forensic/Incident Response Readiness | **Not Addressed** | - Not required |
| Structured Skills Assessments per Job Role | **Not Addressed** | - Not required |
| Process Capability Maturity | **Not Addressed** | - Not required |
| People Capability Maturity | **Not Addressed** | - Not required |
| Incorporates Technical Best practices | **Not Addressed** | - Not required/provided |

| Standard Addresses | ISO 17025 | ISO 17025 Comment |
|---|---|---|
| Provides Assessment tools with Well-defined criteria | **Not Addressed** | • Not required/provided |
| Easy to plan, design, implement, and manage | **Not Addressed** | • Not being specific to digital forensics, problems arise in the interpretation of requirements such as traceability, measurements of uncertainty, and the need for calibration of test equipment. Additionally, the standard state requirements can be open to interpretation, and therefore may result in problems arising in newly formed/accredited labs. |
| Cost of implementation and accreditation | **High** | • Very high cost of implementation and accreditation. |
| Industry Benchmarking for Lab and Personnel | **Not Addressed** | • Inter-lab comparison of results is used for the lab. |
| Well-defined assessment tools and model | **Not Addressed** | • Too generic and not focussed on subject matter. Open to interpretation by the assessor. |
| Adaptable and readily expandable | **Not Addressed** | • Not covered. |
| Proprietary licensing model for use and access to standard | **Yes** | • All standards and contributions by member states are owned by ISO. |
| Annual review and update lifecycle | **Not Addressed** | • Standards generally reviewed every five years; however, ISO 17025 was last updated in 2005 (more than ten years ago at the time of writing). |

ISO 17025 provides a means to assess laboratories, not functions, whereas it is predicted that in future, organisations will need a means to assess and compare the compliance and performance of digital forensics labs, and the various defined functions within them through capability maturity.

The need for a new, more proactive model for establishing, planning, and implementing the running, auditing, and assessing digital forensic labs was drawn out of reviews of issues related to ISO 17025, feedback from practitioners, feedback from business unit owners, and reviews of some of the practical issues encountered and limitations of ISO 17025 in digital forensic labs.

The ability to define and measure capability maturity is important, as a means of benchmarking performance and improvement across the three key areas of digital forensics namely: People, Processes, and Tools. Most digital forensic models focus on a specific aspect mainly related to processes; none look at digital forensics from a holistic perspective taking into account business, technical, and maturity capability requirements.

Overall, while ISO 17025 provides a foundation and starting point that can be applied to digital forensic labs. However, ISO 17025 does not factor process, people, and organisational efficiency into its requirements, and therefore does not address capability maturity or operational efficiency issues those digital forensic labs today face. It is best suited to legacy testing labs, and as a result may fall short of fully addressing the requirements of emerging sciences such as digital forensics. This standard is fast becoming outdated and may soon prove to be too dated and rigid to be effective for addressing the multitude of challenges that digital forensic labs face today.

## 2.4 CAPABILITY MATURITY

### 2.4.1 Performance, Process Improvement, and Maturity

Measuring performance of a digital forensic laboratory has, until now, been very subjective, based on previous experience and as witnessed during various interviews and instances of feedback from participating labs. Previous experience showed that most Performance measurements and managerial Key Performance Indicators (KPIs) within most digital forensic labs tend to focus on items such as:

- Conformance to agreed Service Level Targets (SLTs),
- The number of cases or devices received/examined, and
- The volume of data processed over a given reporting period, etc.

Realistically, of these common KPIs chosen by organisations, only Service Level Targets (SLTs) are critical KPIs that can provide areal indication of performance. SLTs, are perhaps the only performance objective (of those listed above) that can be governed and regulated by a digital forensic lab, and be used as a realistic indication of performance. The other typical KPIs are dependent on customers and volume of data, neither of which the lab has any real control over, and have no direct indication as to levels of maturity, quality, or capability. However, these 'false' performance indicators are often touted as being indications of a lab's performance, and as a yardstick to indicate improvements/efficiency. Service Level Targets are vital KPIs used to help determine overall capability maturity and service levels to customers, and this may be done in conjunction with other KPIs such as volume of data analysed.

Process improvements can be achieved by devising accepted methods to measure processes, and their outputs and results. These distinct steps are critical to any improvement strategy. Lord Kelvin theorised that achieving efficiency via performance improvement is the process of evaluating a given process, or a set of processes, and then determining how the process can be improved to help achieve greater efficiency, quality, or output (Thompson, 1910). Performance measurement is 'the process of quantifying the efficiency and effectiveness of past actions' (Neely, 2002). In contrast, some would define it as 'the process of evaluating how well organisations are managed and the value they deliver for customers and other stakeholders' (Moullin, 2002). Both Neely and Moullin provide valid insights into how performance management is best achieved, and insights from Neely and Moullin were used in the formulation of the research methods and assessment tool used during this research.

The fundamental *improvement process* as defined within Humphrey's Maturity Framework has five basic elements (Humphrey, 1987):

1. An understanding of the current status of the development process,
2. A vision of the desired process,
3. A prioritised list of required improvement actions,
4. A plan to accomplish these actions, and
5. The resources and commitment to execute the plan.

Whilst the 'Maturity Framework' that Humphrey defined was aimed at software development processes, the same principles were used in the formulation of the widely used SEI Capability Maturity Model (CMM), and was later adapted in the People Capability Maturity Model (P-CMM) (Curtis, 2009).

Humphrey's Maturity Framework provided five maturity levels identifying the key improvements required at each level, and established a priority order for implementation. The key lessons that can be gleaned from Humphrey's Maturity Framework that are applied to the CMM can be summarised as follows: 'In addressing problems, treat the entire cycle as a 'collective process' which can be controlled, measured, and improved rather than looking at each process individually, as any effective process must take into account the inter-relationships of the individual processes, people, tools and organisational drivers' (Humphrey W. S., 1987). Many of the digital forensic models and frameworks reviewed focused on specific process aspects of digital forensics; none focused on digital forensics as an all-encompassing collection of interrelated elements, namely People, Processes, and Tools.

Reinforcing Kelvin's rule on measurement and improvement (Nuseibeh & Easterbrook, 2000) the SEI Maturity Framework states, 'The basic principle of process management is that if the process is under statistical control, a consistently better result can only be produced by improving the process. If the process is not under statistical control, no progress is possible until it is under statistical control'. The need to be able to measure performance and the level of maturity is a key organisational and business requirement for all types of organisations that have implemented quality management/business improvement strategies. Decision-makers and senior practitioners are looking to measure various, if not all, aspects of the digital forensics operations with the view of optimisation and quality improvement - all of which should equate to cost reduction.

### 2.4.2 Quality and Capability Maturity Inter-Relationship

The CMM is based on the Process Maturity Framework first described in *Managing the Software Process* (Humphrey, 1989). The CMM incorporates key elements of the Process Maturity Framework, and the Quality Management Maturity Grid (QMMG) was first introduced in *Quality is Free* (Crosby, 1979). In this book, Crosby theorised that by applying QMMG to business processes, the potential gains from quality management would offset any associated long-term costs of effectively implementing and maintaining such a quality management system (Crosby, 1979), a view still held by many quality management practitioners today.

Later, Humphrey built on Crosby’s Maturity Framework and incorporated aspects related to stages of development and progress that organisations would graduate through as they implemented quality management systems and processes. The five stages are the five levels now commonly referred to as the CMM Levels of Maturity.

The Capability Maturity Model (CMM) and its various derivatives today are based on the Deming Model for Improvement (Anderson, Rungtusanatham, Schroeder, & Devaraj, 1995), and the subsequent derivatives of that model, coupled with the basic principles of improvement and assessment as first outlined by Bacon (Bacon, 1620). CMM lends itself well to the various aspects of quality management across all facets of digital forensics philosophy.

### 2.4.3 Critique of Capability Maturity Models

Maturity models are popular tools used for a variety of tasks such as to rate capabilities of a manufacturing process, and to identify elements to help increase the overall level of maturity for that process.

The term ‘maturity’ relates to the degree of formality and optimisation of processes. On the methods used to create the models, Kohlegger et al. rightly criticised that ‘Many maturity models simply and vaguely build on their often well-known predecessors without critical discourse about how appropriate the assumptions are that form the basis of these models’ (Kohlegger, Ronald, & Stefan, 2009).

In its simplest form, a maturity model provides:

- A means to define tasks and processes
- A means to quantify/rate efficiency
- A common language and shared goals/vision
- A framework for prioritising and rating actions
- A way to identify methods to improve overall maturity rating

In Capability Maturity Model v1.1, the authors stated that they created a maturity questionnaire to provide a simple tool for identifying areas where an organisation's software process needed improvement. Rather unexpectedly for the authors, the maturity questionnaire was regarded as 'the maturity model', rather than its intended goal, which was to provide a tool to assist with exploring process maturity challenges and opportunities (Paulk, Curtis, Chrissis, Weber, 1993).

In CMM for Software v1.1, Paulk et al. highlighted that the key criteria for defining process improvement goals require a detailed understanding of the differences between mature and immature processes, and their related business units. Paulk et al. found that within organisations that were found to be immature, the absence of established, mature processes resulted in methods and processes being improvised and applied in an ad hoc manner (Paulk, Curtis, Chrissis, Weber, 1993). Additionally, they discovered that within an immature organisation there was no rational objective basis upon which they could assess and remediate process problems and effectively measure quality. The result invariably was that the lack of consistency affected the quality of products and operational capacity. Practitioner/end user input is key to counter this common pitfall in the design and optimisation of processes.

Key principles of CMM for Software that can be applied to digital forensic processes are that 'The CMM was designed to guide organisations in selecting process improvement strategies by determining current process maturity and identifying the few issues most critical to quality and process improvement. By focusing on a limited set of activities and working aggressively to achieve them, an organization can steadily improve its organization-wide process to enable continuous and lasting gains in software process capability' (SEI, 1993).

A CMM is essentially a framework for helping to guide an organisation from one that lacks process maturity, and therefore is most likely to be affected by efficiency problems, to a well-structured, mature, and efficient business entity. Use of such a model is a means for organisations to bring their practices under a more scientific system of process control and evaluation in order to help rate and possibly improve their overall efficiency. CMMs should identify and document what tasks should be performed, and in what sequence in order to 'help define, manage, monitor, and improve the organization's process(es) rather than exactly how the specific activities must be performed' (US Patent No. 2006/0069540 A1, 2006).

CMM was originally designed to help improve software development processes, but can be applied to other processes and systems equally as well (Paulk, Curtis, Chrissis, Weber, 1993). Ideally, CMM should be applied to all processes in order to help determine the current maturity levels per task, unit, and section, and then to look at methods, tools, etc. that could be used to help improve the maturity level per task, section, or unit, and ultimately for the digital forensic lab overall. Integrating CMM with ISO 17025 documented processes and procedures works well in that ISO requires a documented set of processes to be defined for every task performed during an examination. By using CMM, the quality of ISO-related documentation could be improved without making the documented processes too unwieldy and complex.

Within the context of CMM, *process capability* refers to an organisation's potential to meet a specification/rating or level or maturity. *Process performance* is the measure of actual results of a specific task that may or may not fall within the required or accepted maturity level.

Process maturity can be used as a reliable indicator of the level to which a specific process has been defined, managed, how it can be measured, how it is controlled, and overall how effective a given process is (US Patent No. 2006/0069540 A1, 2006).

#### 2.4.3.1 People Capability Maturity Model (P-CMM)

The Carnegie Mellon University Software Engineering Institute originally developed the People Capability Maturity Model (P-CMM) in order to assist businesses in better identifying and managing knowledge workers, their support processes, and the wealth of knowledge within their respective business units and organisations. Similar to CMMI, P-CMM has five maturity levels. However, it is focussed more on the need to improve the capabilities of workforce/skills as a differentiating factor from the competition (Executive Brief, 2009).  P-CMM is equally important to achieving efficiency in digital forensics as is process CMM.

Justification for including P-CMM within digital forensic processes and strategies is that P-CMM was created to help develop and mature employees' competencies and proficiency and therefore lends itself well to the requirements of digital forensics personnel based on ISO 17025 and ASCLD-LAB requirements.

In order to maximise the benefit of employees’ technical knowledge to achieve greater business efficiency, staff development and improvements have a direct bearing on the company’s efficiency ratings, and business processes.  Improvement in business processes without corresponding staff (people) efficiencies does not allow for an environment conducive to maximising overall process efficiency and maturity.

The People Capability Maturity Model (P-CMM) is a tool and management approach utilising the Capability Maturity Model for Software (SWCMM) process maturity framework as its foundation to enable the establishment of best practices for better defining, measuring, ‘managing and developing an organization’s workforce’ and enables an organisation to identify and address key aspects related to people and skills within an organisation (Curtis, 2009).

Curtis defined the People Capability Maturity Model (P-CMM)’s design goals as assisting organisations in better (Curtis, 2009):

- Defining the maturity of their workforce practices,
- Establishing a programme of continuous workforce development,
- Setting priorities for improvement actions,
- Integrating workforce development with process improvement, and
- Establishing a culture of excellence within the organisation.

When examining the pitfalls of many approaches to quality and maturity improvement, Curtis et al. theorised that by using the P-CMM framework, that organisations could avoid introducing workforce quality management practices that its employees were unprepared, or unskilled, to implement effectively (Curtis, Hefley, & Miller, 2002).

Curtis’s P-CMM key points are:

- Each process area comprises a set of goals that, when satisfied, stabilise or improve an important component of workforce capability.
- Each process area is described in terms of the practices that contribute to satisfying its goals.

Essentially, P-CMM provides a roadmap to help transform an organisation to become more efficient through a system of steadily improving its workforce practices and employee skills. The People CMM, like other CMM models, consists of five maturity levels, through which an organisation’s workforce practices and processes evolve. At each maturity level, a new system of processes or practices is added to those implemented at previous CMM levels. Similar rating for software CMM exist, but have limited relevance to this discussion at this stage. Table 2 provides a sample of the process maturity ratings applicable to CMM and P-CMM.

Table 2: Process Maturity Ratings

| Maturity Level | Person-Dependent | Documented Process | Partial Deployment | Full Deployment | Measured & Automated | Continuously Improving |
|---|---|---|---|---|---|---|
| Level 0<br>Person-Dependent | Yes | – | – | – | – | – |
| Level 1<br>Documented Process | – | Yes | – | – | – | – |
| Level 2<br>Partial Deployment | – | Yes | Yes | – | – | – |
| Level 3<br>Full Deployment | – | Yes | – | Yes | – | – |
| Level 4<br>Measured & Automated | – | Yes | – | Yes | Yes | – |
| Level 5<br>Continuously Improving | – | Yes | – | Yes | Yes | Yes |

Curtis et al. defined *workforce capability* as the levels of ‘knowledge, skills, and process abilities available for performing an organization’s business activities’ (Curtis, Hefley, & Miller, 2010). The elements addressed by any system aimed at improving workforce capability would be knowledge, skills, and process maturity.

P-CMM’s primary objective is to improve organisational workforce capability. Workforce capability indicates an organisation’s:

1. Readiness in performing its critical business activities,
2. Likely results from performing these business activities, and
3. Potential for benefiting from investments in process improvement or advanced technology.

Ideally, most organisations strive to plan their workforce, their skills, and core competencies to meet their business goals and drivers (Prahalad, 1990). Prahalad stated that in order to measure and improve capability, various tasks need to be performed. The tasks referred to were:

a) The personnel should be divided into various roles based on required competencies.

b) Each competency should be represented as a unique task through which the required knowledge, skills, and processes could be incorporated via specialised training and/or work experience.

### 2.4.4 Capability Maturity Summary

Capability Maturity is a key element and part of the unique aspect of the proposed digital forensics model. CMM in its various forms is viewed as an ‘elective’ system that some organisations (mainly in the manufacturing sectors) may choose to implement. The very nature of digital forensics labs today is faced with growing case-loads, exponential volumes of data to analyse (Goodison, Davis, & Jackson, 2014), budgeting and resourcing constraints, regulatory requirements for accreditation, and the shortage of skilled resources, which make the need for CMM and P-CMM essential for the long-term sustainability and survival of digital forensics laboratories. CMM and P-CMM are also means of contributing towards more ‘well-rounded’ digital forensics practitioners, certifications, and proficiency testing.

CMM and P-CMM will be applied and defined with specific tools and guidelines within the proposed digital forensics model. The proposed model will incorporate a combination of CMM and P-CMM within the assessment, planning tools, and derived feedback and know-how to help organisations improve their CMM via more concise and optimised process documents to be included within proposed digital forensics model knowledge base.

## 2.5 SUMMARY

A detailed review of digital forensics process models was conducted as part of this research, together with a detailed review of digital forensic investigation frameworks. Of the various digital forensic models and investigation frameworks reviewed, none covered the Capability Maturity and Process Efficiency. Each focussed on a specific technical aspect related to digital forensics, with none of the models or frameworks examining digital forensics from a holistic quality management and technical perspective. Capability maturity can, however, be implemented to measure the effectiveness of any process or sub-process, and thereby could be applied to these models within the scope of the proposed digital forensics model.

Addressing technical issues in digital forensic models without addressing non-technical issues related to Organisation, People, and Processes, including capability maturity, seems to be a common pitfall of many of the digital forensic models and frameworks assessed to date. Technical and non-technical challenges cited in the various digital forensic models and frameworks reviewed are presented in Table 3; each challenge is represented by a check mark (✓).

Within this table, the perceived challenges facing digital forensic labs are listed together with reference to any exiting model or framework that addresses that challenge. Each challenge is categorised as being a People, Process, or Tools issue, and the names of the models that refer to or address the challenge are listed for each of the 19 key challenges identified.

## Table 3: Mapping and quantifying digital forensics challenges

| Digital Forensic Challenges | DF-$C^2M^2$ Category | | Organisational | Process | People | Tools & Methods | Cited As a Challenge By |
|---|---|---|---|---|---|---|---|
| | Type of Challenge | | Legal & Regulatory | Standards & Best Practices | Training & certification | Technological | |
| | | Challenge | | | | | |
| | 1 | Technology Changes/Diversity | | | | ✓ | DFRW, Mohay, Brill & Pollit |
| | 2 | Video and Rich Media (Multimedia) | | ✓ | | ✓ | Cohen |
| | 3 | Encryption | | ✓ | | ✓ | Lindsey, Casey |
| | 4 | Wireless | | ✓ | | ✓ | Lindsey, (Implied Casey) |
| | 5 | Anti-forensics | | ✓ | | ✓ | Lindsey, Casey ** |
| | 6 | Virtualisation | | ✓ | | ✓ | Lindsey **, Casey ** |
| | 7 | Live Response | | ✓ | | ✓ | Lindsey **, Casey ** |
| | 8 | Distributed Evidence | | ✓ | | ✓ | Lindsey **, Casey ** |
| | 9 | Usability & Visualisation | | | | ✓ | Lindsey **, Casey ** |
| | 10 | Volume of Evidence (Data) | | | | ✓ | Mohay et al., Lindsey |
| | 11 | Education & Certification | ✓ | | ✓ | | Mohay et al. |
| | 12 | Embedded Systems | | | | ✓ | Mohay et al., Lindsey ** Casey ** |
| | 13 | Forensic Readiness | | ✓ | ✓ | | Mohay et al. |
| | 14 | Monitoring the Internet (Intelligence) | ✓ | ✓ | ✓ | | Stephenson |
| | 15 | Tools (Development, Testing) | ✓ | ✓ | | ✓ | Lindsey **, Casey ** |
| | 16 | Networked Evidence | | ✓ | ✓ | ✓ | Stephenson |
| | 17 | Adapting to Shifts in Law/Regulatory | ✓ | ✓ | | | Spafford, Casey, McKemmish, Ciardhuain, Kohn et al. |
| | 18 | Developing Standards | ✓ | ✓ | | ✓ | Lindsey |
| | 19 | Capability Maturity | ✓ | ✓ | ✓ | | Krutz |

**Legend:**

**** indicates implied by a broader statement, but not explicitly mentioned by name.**

This research aims to prove that capability maturity can extend to the various frameworks and models via a well-defined set of CMM-oriented process definitions, key performance indicators (KPIs), process refinements, and restructuring or some organisational goals. The Digital Forensics – Comprehensive Capability Maturity Model (DF-C²M²) seeks to address the challenges identified during this research and from this literature review through its incorporation of capability maturity through all three key organisational elements, namely: People, Processes, and Tools.

The critical success criteria for implementing capability maturity within a digital forensics lab would include:

- An established of well-defined technical and operational policies and procedures that integrates the CMM, and P-CMM requirements within the core processes and Key Performance Indicators (KPIs).
- Development of a method/tool measure to assess and measure ISO 17025/ASCLD-LAB compliance and CMM across the People, Process and Tools domains of the organisation.
- Detailed skills profiles per task and well defined training progression and skills matrices
- A detailed services catalogue that clearly identifies the skills, tools, processes and prerequisite requirements for the effective delivery of each service.
- A means to benchmark and compare CMM KPIs for various labs within the same sector
- An established digital forensic, CMM-centric, and ISO 17025 compliant Body of Knowledge that enables an organisation to relatively quickly implement the required policies, procedures and controls for CMM effective operations.

Throughout the research and reviews completed to date, it has been apparent that although a multitude of digital forensic process and investigation models exist, none fully address the complete set of Process, People, and Technology aspects of digital forensics. Gaps within existing standards and opportunities for improvement by augmenting the requirements of such standards have been identified.

Taking into consideration key criticisms and pitfalls of current standards, and processes and problems faced by digital forensic labs and practitioners, and in view of the fact that no single, existing digital forensic model addresses the requirements of growing and emerging digital forensic labs, it is clear that an opportunity exists to define a new digital forensic model and a capability maturity framework, to address the requirements of digital forensic laboratories and regulators alike.

The proposed model would provide a universal set of criteria by which digital forensic laboratories could be assessed, accredited, and improved (via elements of a Capability Maturity Model (CMM)), and assist towards the global recognition of the specialist field of digital forensics. The proposed model would contribute towards a more well-defined set ready to use best practises, policies and procedures ready aligned to prevailing ISO 17025, ASCLD-LAB and other related digital forensic standards. Additionally, the model would provide more detailed and structured digital forensics-specific career progression, proficiency testing criteria, and provide a global framework based upon which digital forensic laboratories, their processes, tools, and personnel could be benchmarked against comparable other laboratories with the ultimate goal of improving efficiency, quality processes, and proficiency of digital forensic personnel through the integration of capability maturity across all three domains.

The proposed model would thus provide a means by which local and international governing bodies could accredit, vet, and possibly even license digital forensic laboratories and personnel in their jurisdictions, and thereby provide the benchmark for rating and accrediting digital forensic laboratories and practitioners and thereby, help to improve the quality, and credibility of digital forensics as a true scientific profession.

# CHAPTER 3: DF-C$^2$M$^2$ - PRACTITIONERS SURVEY, INTERVIEWS and WORKSHOPS

## 3.0 INTRODUCTION

Practitioners input and feedback were critical aspects of this research, initially to help gauge challenges faced across the board, to determine critical requirements to achieve capability maturity within digital forensics, and as a means to test and refine the model, the assessment tool, and the key elements of the body of knowledge.

Key aspects of design process elements included:

1. Conduct surveys, interviews, assessments and consultations with participating digital forensic practitioners, managers, and investigators.
2. Analyse feedback and findings.
3. Conduct workshops and seminar on draft DF-C$^2$M$^2$ for review, and solicit feedback and areas for improvement from interviewees.

Practitioner feedback and involvement during this research was achieved through:

1. Online survey of challenges and issues related to digital forensics training, proficiency, capability and quality management,
2. Practitioner Interviews on challenges, and possible solutions,
3. Participant labs DF-C$^2$M$^2$ introductory workshops,
4. Lab assessments,
5. DF-C$^2$M$^2$ model review, evaluation and feedback.

### 3.1 ONLINE SURVEY OF PRACTITIONERS

An online survey was created to solicit feedback from practitioner regarding the present training, proficiency and skills issues affecting digital forensic laboratories. Participants were solicited via an online forum, and invitations were sent to possible participants via email.

The survey yielded 57 participants 34 of whom completed all questions from 14 countries [3] who provided input as to the main issues related to digital forensics as a

[3] For details of participant countries – see Appendix C

profession, issues related to training, skills and the need for a common body of knowledge. The information gathered provided a useful foundation in helping to structure and determine the foundational elements of the DF-C²M² People domain, and provided insight into issues not full addressed by existing accreditation requirements.

**People:** Issues related to competency testing and proficiency testing were explored and both were found to be lacking and in need of improvement. Opinions were sought on current digital forensics training offerings and approaches and some of this information was used to enhance the draft DF-C²M² skills matrices and career progression training paths. The decision to include cybercrime within the scope of the DF-C²M² was taken as the majority of participants felt that there was an overlap between digital forensic examinations and cybercrime investigations, but also because the 75.6% of the participants felt that technical knowledge of how cybercrimes are perpetrated are key to helping develop a more comprehensive digital forensics examiner/practitioner.

Participants felt that present academic training had not sufficiently provided those with the skills need to be able to work as digital forensic practitioners with 73.7% requiring additional training after having completed education in digital forensics related degrees at university. This highlighted the need for a more rigorous training progression path for various roles within a digital forensic lab, and the need for skills matrices to help assess gaps in knowledge and skills as part of the People domain. All of the issues raised by participants could have an impact on the quality of services, proficiency, and capability maturity of personnel.

Participants viewed a practitioner capability as being dependant on their experience, competency and results of proficiency, though none identified conformance with service levels, and benchmarking within a lab as a means of determining capability, nor the use of P-CMM as an option. The majority of participants (42.1%) felt that there was a need for a new model to assess and evaluate capability of digital forensic practitioners.

**Process:** 80% of respondents indicated that their organisations had policies and procedures related to digital forensics and 68.6% indicated that these include some form of quality management processes/systems. 62.9% of respondents reported that their present quality management system in reviewed for relevancy at least once every three years. Analysis of the comments revealed that documentation is part of existing quality systems, but depends on efficiency of individuals in the organization.

**Tools:** As to whether the organisation maintained system for validation and verification of tools; the majority of respondents (77.1%) replied positively. and 11.4% answered were not sure. This indicates existence of documentation of results from validation testing on tools used in the acquisition of digital evidence.

As to whether the organisation used some form of best practise for digital evidence handling; 88.6% responded yes. Analysis of comments revealed the use of APCO and ISO best practice/standards.

**Capability:** When asked if the new capability model should focus exclusively of digital forensic specialists (People) or include other types of capability maturity, of the thirty-eight participants that responded; 21.1% recommended Only Digital Forensic Specialist (people) maturity, 15.8% recommended other types of maturity and 63.2%, were not sure. This possibly indicates that the majority were confused. Which could possibly be attributed to a misunderstanding between the terms Model vs. Maturity, or to some kind of resistance to the idea of assessing and enforcing through a new capability model perhaps feeling that this would potentially jeopardise job security of some participants. Analysis of the comments revealed a possible resistance of new approaches and the term "model" was confusing to those who sought a renewed approach as well as those who did not want any change and prefer the status quo. A common Body of Knowledge specific to Digital forensic perhaps could help address any confusion of reservations displayed – this opinion was supported by practitioners involved in the workshops and evaluations.

The finding and results of this survey gave insight into additional areas that should be included within the scope of the project, and validated that the main areas of concern amongst practitioners could be categorised as People, Process, Tools and Capability.

## 3.2 PRACTITIONER INTERVIEWS ON CHALLENGES, AND POSSIBLE SOLUTIONS

**Participating Laboratories' Background Information**

Two labs volunteered to participate in the research, and the total number of participants from the participating labs was 20 drawn from a cross-section of students, forensic trainees, examiners, senior examiners, consultants and lab managers. Permission and participation was obtained from the heads of the two volunteer digital forensics labs to interview personnel, and conduct an assessment of the processes and personnel and participants completed the Participant Consent Form (Appendix B). A summary of the laboratories is listed in Table 4:

**Table 4: Summary of participating labs**

| # | Referred to As | Industry or Sector | ISO 17025 or ASCLD/LAB Accredited. | Number of Years in Operation |
|---|---|---|---|---|
| 1 | LAB #1 | Law Enforcement | Yes | More than 3 years |
| 2 | LAB #2 | Academic | No | 1 year |

For each participating laboratory, details of the total number of personnel and roles was documented as reflected in Table 5, and the details of those who participated in the assessments, interviews, and feedback are highlighted in Table 6:

**Number of Lab Personnel by Function** (as of the time of assessment):

**Table 5: Number of personnel by function in participating labs**

| Lab Id | Lab Manager/ Director | Deputy Lab Manager | Health & Safety Manager | Senior Forensic Examiner | Forensic Examiner | Forensic Engineer/ Technician | Other | Total |
|---|---|---|---|---|---|---|---|---|
| Lab #1 | 1 | 1 | 1 | 3 | 7 | 5 | 4 | **22** |
| Lab #2 | 1 | 1 | 1 | 1 | 3 | 2 | Varies | **9** |

Table 6: Assessment, audit, and interview participants

| Lab Identifier | Role | No. of Related Years' Experience | Feedback on DF-C²M² |
|---|---|---|---|
| Lab #1 | Lab Director | 5+ | Y |
| Lab #1 | Lab Advisor | 5+ | Y |
| Lab #1 | Senior Forensic Examiner | 5+ | Y |
| Lab #1 | Forensic Examiner | 3 to 5 | Y |
| Lab #1 | Forensic Examiner | 3 to 5 | Y |
| Lab #1 | Forensic Engineer | 1 to 2 | Y |
| Lab #1 | Forensic Engineer | 1 to 2 | Y |
| Lab #1 | Advisor | 5+ | Y |
| Lab #2 | Lab Director | 5+ | Y |
| Lab #2 | Forensic Examiner | 1 to 2 | Y |
| Lab #2 | Forensic Engineer | 1 to 2 | Y |
| Lab #2 | Student A | Less than 1 | Y * |
| Lab #2 | Student B | Less than 1 | Y * |
| Lab #2 | Student C | Less than 1 | Y * |
| Lab #2 | Student D | Less than 1 | Y * |

**Disclosure:** The researcher had previously served as project director for the project in which Lab #1 was designed, built and implemented. However, of the original Lab #1 team that were included in the evaluations and workshops, only one participant had a previous direct working relationship with the research during his tenure as lab project director. All other lab #1 participants were chosen based on the fact that they had not worked nor reported to the researcher, and none of the Lab #1 participants had any reporting lines to the researcher at the time of the research.

**Note *:** A small number of academic students from the university were included in the review of the DF-C²M² Body of Knowledge to gauge whether they found the Body of Knowledge content to be beneficial for newcomers to the profession. The majority identified the Body of Knowledge Technical Manual, procedures, and workflows as being the most useful and beneficial.

Having developed the core DF-C²M² framework which consisted of the initial technical workflows, process documentation, assessment tool and first draft of the body of knowledge, the first step was to interview participants on the perceived challenges and issues related to digital forensics. These interviews were conducted in person and audio recordings were made with participant agreement, with the majority of participants agreeing to have the interviews recorded. Participants were also taken through the questions used in the online survey and the answers were noted and recorded. The face-to-face interview provided the researcher with the ability to drill down in certain areas and solicit more information and gain insight into the perceived challenges, the underlying causes and possible solutions. Most the interviews lasted about an hour, with some the more experienced personnel taking up to 3 hours to complete the interview and related discussions. Questions asked during the interviews and workshops included:

1. Questions from the online survey

2. Questions related to perceived personnel, process and tools challenges. For these questions, participants were asked:

    a. What the challenges and the lab face regarding ISO 17025 compliance?

    b. What shortfalls or gaps did they believe exist within the current system processes?

    c. How did they believe the issues could be best addressed?

    d. What issues did they perceive in the lab trying to measure compliance and identify its gaps?

    e. Were best practices implemented and if so, where these documented and auditable?

    f. What short coming existed within the current regime of competency testing and skills development, and how did they believe these could best be addressed?

    g. Was planning for /and or implementing ISO 17025 resource consuming and if so, which resources were most affected by such efforts?

From these interviews, the participants' main concerns could be categorised as being related to the People, Process and Tools organisational elements. At this stage, participants were not yet aware of the DF-C²M² model, the Body of Knowledge nor what it contained. In many ways, these interviews helped to affirm the original research assumptions about challenges, and introduced new issues such as the need for performance management (later categorised as being related to Capability Maturity).

## 3.3 PARTICIPANT LABS DF-C²M² INTRODUCTORY WORKSHOPS

DF-C²M² introductory workshops were held with participants from two participant labs. The workshops began with a broad discussion on challenges as they related to the People, Process and Tools domains. Next, the DF-C²M² was introduced with the key design goals and the objectives of the research. Participants were presented with summarised results of the surveys, and interviews and initially presented

The workshop covered eight key areas:

1. Discussion on Digital Forensic Challenges (including those identified by participants in 3.2)
2. DF-C²M² goals
3. DF-C²M² Service Catalogue
4. DF-C²M² People Domain
5. DF-C²M² Process Domain
6. DF-C²M² Tools (and Methods) Domain
7. DF-C²M² Assessment Tool
8. DF-C²M² Body of Knowledge Review

As part of these workshops; participants were shown key elements of the model and asked for feedback on its relevance, suitability, practicality, and how they believed it could be improved. Participants were also asked about how best to assess lab compliance with ISO 17025 and Forensics readiness in general, and then introduced to the assessment tool. The core discussion at this phase centred on key elements of measuring forensic readiness, how to measure ISO 17025 compliance, and how capability maturity or 'performance management' challenges presently not covered within existing standards and best practices has been implemented within the model and its assessment tool.

Skills and training was introduced amongst the main issues previously raised and the proposed sample solution of the skills matrix and training progression plans were introduced with and introduction to the concept of People Capability Maturity and what P-CMM entailed within the context of digital forensics. The assessment tool was introduced and participants were taken through the use of the tool, the service catalogue and sample assessment results, and how these could be remediated through the DF-C$^2$M$^2$ body of knowledge. Participants were taken through each aspect of the assessment tool and shown how capability maturity had been integrated within the model and the assessment tool.

At each stage of the workshops, interviews and assessments, participants were asked for feedback and provide suggestions on how the present DF-C$^2$M$^2$ key elements could be improved. The DF-C$^2$M$^2$ Body of knowledge was introduced and participants were taken through the design goals, the contents, workflows, and a discussion around its suitability. A softcopy of the DF-C$^2$M$^2$ Body of Knowledge was also made available for detailed review to volunteer participants from each lab. These volunteers were given a week in which to review of the Body of Knowledge in detail, and provide feedback on its relevance suitability, practicality and any gaps identified.

Throughout this research where key design/or element decisions were made based on participant feedback or consensus – this is duly noted. Upon completion of the workshops, they lab assessment and the DF-C$^2$M$^2$ reviews, DF-C$^2$M$^2$ evaluation forms were distributed to participants. These forms were collected a week later from the lab managers after participants were given time to review softcopies of the DF-C$^2$M$^2$ Body of Knowledge.

Some participants volunteered to participate in the labs and skills assessments and to review the Body of Knowledge in detail. Interestingly the most valuable comments of ease of use and usability came from the least experienced participants, whilst the most valuable feedback on how suggestions for inclusion or improvement s on the DF-C$^2$M$^2$ came from eth more experienced and managerial participants. The Body of Knowledge was found to be sufficiently detailed by the majority of the participating practitioners to enable a lab to implement it in its entirety with less effort that building such as compendium themselves to achieve accreditation compliant status. While some practitioners felt the Body of Knowledge should be less detailed (in the Process Domain section), others felt the level of detail was prescriptive and suitable for its intended purpose.

## 3.4 DF-C²M² - INTERVIEW AND QUESTIONNAIRES

The DF-C²M² Interviews were conducted face-to-face and recorded in the form of written notes, and audio recordings. The Interview questions included:

- Question from the online survey
- Opinions regarding professionalism with digital forensics.
- Digital Forensics as a Scientific discipline (barriers and dichotomies).
- Training and Certification vs Competency and Proficiency.
- The need and issues related to Digital Forensics standards.
- Limitations of currently applied/adopted digital forensic standards and best practices.
- Issues related to People, Process and Tools
- Issues related to the drive for greater efficiency and capability maturity.
- Feedback regarding current Digital Forensic academic offerings and shortcomings.
- Planning and organisational issues typically faced by Lab Managers
- Reviews of draft DF-C²M².
- Opinions and feedback on draft DF-C²M² model.
- Other feedback and comments related to Digital Forensics.

## 3.5 LAB ASSESSMENTS

For each area being assessed, the assessor also factored in Maturity Level ratings per section. For each organisation type (law enforcement vs. non-law enforcement), the following DF-C$^2$M$^2$ requirements were revised during the workshops via a series of interviews, GAP analysis workshops. For each assessment, a review of the organisation’s digital forensics strategic plan and operational documentation: Services Provided - Service Catalogue(s) and Known Service Dependencies (People, Processes, and Tools), this included:

1. Forensic Readiness Assessment (People, Processes, and Tools)
2. Assessment results summary for addressing the DF-C$^2$M$^2$ People, Processes, and Tools requirements.

DF-C$^2$M$^2$ Assessments using DF-C$^2$M$^2$ were performed for both participating labs using the DF-C$^2$M$^2$ assessment tool to guide the approach to the assessments. Competency testing and witnessing of tasks for the creation of a skill/task analysis was requested by one of the labs, and performed by witnessing and documenting the task analysis with volunteer personnel at that lab performing various digital forensic-specific tasks. Details of the assessment process, findings participating labs, personnel and assessment findings are discussed further in Chapter 5.

# CHAPTER 4: DF-C²M² - PARTICIPATORY DESIGN

## 4.0 – INTRODUCTION

Practitioner involvement was sought via surveys, interviews, lab workshops, assessments and during the model evaluation. Practitioner's involvement in this research was strategic and important as a means of validating decisions, and the practicality of implementing the model. More importantly practitioners were involved at various levels in helping determine the challenges and issues, and verifying those against what was previously assumed at the start of the research. Practitioners from the participating labs were also involved in helping refine possible solutions or improvements on the way their exiting processes worked, and how these were implemented within the model. Practitioner involvement was key to the original ethos of the model to create a sustainable model and body of knowledge supported and maintained by a community of practitioners for the collective benefit of those practitioners and the labs they represent.

Whilst not conforming to any specific participatory deign method per se, practitioners were involved to initially via the online survey help identify challenges towards professionalism within the discipline, and help identify which organisation domains were affected namely People, Process and Tools. The issues of performance and capability maturity were identified at the very beginning as challenges, and this re-affirmed the original research idea that capability maturity within digital forensic was a challenge, but that it also presented a unique opportunity to find a way to incorporate capability maturity within the three organisations domains.

The participatory design (Sanders, 2008) aspects applied within this research involved a cross section of practitioners and lab support personnel all of whom participated to some degree in the consultative interviews, workshops, assessments and the final review and evaluation of the model. Participating practitioners provided an element of peer review of the design objectives and research deliverables and provided insight that helped determine possible gaps within the model, and how best certain aspects of given processes such as the assessment could best be achieved in their view.

Leveraging the feedback from participants enabled rapid refinement of various aspects and elements of the model, and facilitated inclusion of elements not previously considered such as service prerequisites (within the Services Catalogue), and the need for a task/skill analysis for each task performed as part of a typical digital forensic examination.

## 4.1 DESIGN AND DEVELOPMENT USING PARTICIPATORY DESIGN

The core design approach involved the use of participatory design elements (Stephenson, 2003) within DSRP in the following key areas of the research:

- Discussing and addressing issues discovered during a SWOT analysis (Hump (Humphrey A. , 2005), through participant interviews, and the lab assessments findings.
- Discussing and evaluating whether or not the modular approach was best suited for DF-C$^2$M$^2$, and what if any were the limitations of such approach, and what were the advantages?
- How to best incorporate SMART criteria into the design and the assessment tool (Doran, 1981), and whether or not the sample weights and scores assigned in each area were justifiable and appropriate.
- Whether incorporating the Capability Maturity Model (CMM) and People Capability Maturity (P-CMM) (Curtis, Hefley, & Miller, The People Capability Maturity Model: Guidelines for Improving the Workforce, 2002) goals into the design of components of the solution was essential and practical.
- Relevance, and completeness of the model, the assessment tool and the Body of Knowledge.

The model is based on GNU/‘open source’ principles – where the digital forensics community at large is able to use the model and its elements, and are also invited to help improve, refine, and assist in the long-term sustainability and relevance of the model as a ‘peer-reviewed’ model created and contributed to by the community. Participatory design is therefore key to the long-term viability, and acceptance of the model and its key elements.

### 4.1.1 Demonstration

The model has been designed and implemented in part through a series of assessments using the model and tested against the research problem statement and objectives. Participants reviewed the key elements of the model during assessments, interviews, and reviews and provided feedback on relevance, effectiveness, suitability and how elements could be improved.

### 4.1.2 The Assessment Process

As part of this research, digital forensic laboratories were sought for participation in the DF-C$^2$M$^2$ interviews and assessments as part of the participatory design ethos. Due to sensitivities around permitting external researchers to evaluate internal lab process several labs approached were not able to participate. Two digital forensic laboratories that expressed interest in participating in the research and in evaluating the proposed Model were selected due to geographic practicalities. The two volunteer labs were interested to determine DF-C$^2$M$^2$ possible benefits to their existing digital forensic lab processes, and to get insight into how they Capability Maturity could be implemented within the digital forensic lab operations.

The necessary permissions were obtained to interview personnel, and their internal evaluate processes as part of the DF-C$^2$M$^2$ assessments. The required Ethics approval from the University of Lancaster had also been previously secured – details of which can be found in Appendix I.

The DF-C$^2$M assessment research method was designed to be executed as a ‘consultative audit’ and would involve:

1. Solicit participants for online survey.
2. Solicit and select suitable volunteer labs to participate.
3. Introductory meeting and overview with key stakeholders.
4. Reviewing processes and documentation.
5. Interviews with key administrative and a subset of select technical personnel.
6. Interactive discovery workshops on DF-C$^2$M.
7. Witnessing tasks and procedures.
8. Review of assessed lab’s customer feedback.
9. Review of any relevant supporting documentation and records.
10. Soliciting feedback on DF-C$^2$M$^2$ from participants.

11. Wrap-up summary meeting (SWOT analysis based on DF-C²M²).
12. Preparation of final report.
13. Presentation of final report to the assessed organisation.
14. Benchmarking the findings for future analysis and comparisons.

### 4.1.3 Evaluation and Communication

The proposed model was evaluated the DF-C²M² in two digital forensics labs to study its effectiveness in assessing the maturity of digital forensics capabilities in real-world scenarios. The evaluation took the form of a 'consultative audits' and was conducted on-site by the researcher. This thesis will present the findings of the research, and how it has been able to address the research problem and objectives, as well as any limitations related to the scope of the research. Reviews of the proposed model were conducted by experienced practitioners in both law enforcement and academic fields.

Based on feedback from participating practitioners; the approach to assessing a lab was refined slightly to make the process a more consultative, and an engaging learning opportunity, therefore providing a means to enable two-way idea and information exchange between the assessor and the interviewees. This approach was found to be a natural progression on how best to proceed and was also highlighted as a key aspect of participatory design by Murphy and Hands (Murphy & Hands, 2012).

This constant feedback enabled evaluation and adjustment of key metrics throughout the practitioner workshops and assessments rather than only at the end of the workshops and assessments. Murphy and Hands defined this evolution in design as the 3E Approach where "this dynamic relationship becomes a trade-off between the designer's Expertise in design, the client's Experience of their business and indeed the user's Engagement in the whole process" (Murphy & Hands, 2012). This provided a more "mutually-engaging" research exercise, which enhanced practitioner participation and provided a collaborative learning and discovery opportunity for all parties involved.

Proof of this is perhaps that while assessments are typically considered as a means to provide the 'client' with feedback and findings, the assessments conducted using the participatory design approach provided invaluable insight into how certain elements with the model could be improved, added or eliminated (due to redundancy) and to help identify elements previously not considered. The assessments therefore proved to be as much a refinement and learning exercise for the researcher as the assessment findings did for the assessed labs.

## 4.2 PARTICIPATORY DESIGN WITHIN DSRP DESIGN STAGES

### 4.2.1 DF-C$^2$M$^2$ Introductory Workshops and Reviews

Participants from each lab attended one of two initial introductory workshops to introduce the DF-C$^2$M$^2$ Framework and design goals. Capability Maturity was introduced and how it should be applied to the People, Processes, and Tools domains of an organisation was described. During this introduction, it was noted that many of the participants had not considered Capability Maturity as a requirement within Digital Forensics. Many participants had assumed that ISO compliance and typical KPIs such as volume of data, number of devices, and cases examined were sufficient indicators of efficiency for the laboratory and/or an examiner.  This finding reaffirmed the theory that ‘false performance indicators’ are often used as measures of efficiency, and by virtue of that, assumed Capability Maturity, as stated in Chapter 1.

Participants were invited to complete the DF-C$^2$M$^2$ survey and list challenges they faced from both a lab management and practitioner perspective. The majority of the challenges stated re-enforced the original DF-C$^2$M$^2$ initial assumptions as defined in Chapters 1 and 2.

### 4.2.2 DF-C$^2$M$^2$ Assessment Tool Review Workshop

Participants were introduced to the DF-C$^2$M$^2$ Framework, Body of Knowledge, and assessment tool. Participants were able to review the standard operating procedures, workflows, and forms. Standard operating procedures and workflows – specifically those related to technical subjects as defined within the Technical Manual -- created the most interest in both groups of participants, understandably as the majority of the participants were technical, which also reflects the general staffing ratio of technical to non-technical staff within most digital forensic laboratories.

For a more comprehensive evaluation of the DF-C$^2$M$^2$, select key personnel from each lab were given copies of the Body of Knowledge to perform a more thorough review and to provide more detailed feedback and evaluation of the DF-C$^2$M$^2$.

Overall, the Body of Knowledge was well-received by technical and non-technical participants alike. Key observations include:

1. The workflows proved to be of most interest to the student participants who found the Body of Knowledge to be ‘voluminous’, possibly reflecting their interest in methods of grasping new content in the simplest and quickest way available – which the workflows helped them to do.
2. Managerial lab personnel were most interested in the Body of Knowledge components related to Lab Operations, Training, Quality Management, Assessment Tool Reports including Skills Matrices, and Capability Maturity Ratings.
3. The ethos of the Digital Forensics Body of Knowledge supported and maintained by a community of practitioners was generally seen as a bonus aspect of the model.

### 4.2.3 DF-C$^2$M$^2$ Assessment Tool – Process and Objectives

Participants were presented with an overview of the Assessment Tool and the Assessment Process. The key stages of the assessment, which were designed to follow those found in ‘conventional’ ISO audits, were followed, and the method used to validate and determine answers was briefly discussed.

Initially, it was thought that the duration of the assessment would require discovery of evidence and that witnessing of tests would require two days for the assessor to complete; however, it was realised during discussions with participants that perhaps three to four days with the fifth day to present findings was probably more realistic (dependent on the size of the lab).

The assessment tool included ISO 17025 audit requirements structured along the lines of People, Processes, and Tools, and it was noted during this presentation that less-experienced delegates needed help on how to assess or address each question or criterion in the assessment tool.

This oversight in the design of the Assessment Tool, which assumed that those using the tool for in-house assessments would be well-versed with standard ISO 17025 audit procedures on how to validate answers or support findings with evidence, meant that tips on what to look for would need to be added to each question/criterion within the assessment tool to help guide the assessor and to address this rather important requirement, as it would affect the ability of newer labs to conduct self-assessments effectively, and thus affect the perceived benefits to newer and less experienced labs.

Based on the feedback from an ISO 17025 digital forensics auditor, it was agreed that existing ISO 17025 and ASCLD/LAB assessors would be able to conduct DF-C$^2$M$^2$ assessments using the Assessment Tool, the existing ISO 17025, and their digital forensics knowledge and experience, and that the DF-C$^2$M$^2$ would facilitate more detailed internal ISO 17025 audit assessments and preparations.

Table 7 identifies key DSRP design stages of the research where practitioners were directly involved:

Table 7: Practitioner Involvement

| | DSRP DESIGN STAGE | Practitioner Involvement |
|---|---|---|
| 1 | An initial problem definition and identification. | - |
| 2 | Defining objectives of the research. | - |
| 3 | Research existing standards, models, and best practices generally used in Digital Forensic Laboratories. | - |
| 4 | Research requirements for accreditation under ISO 17025/ASCLD-LAB and perceive the challenges of attaining and maintaining accreditation. | - |
| 5 | Designing initial DF-C²M² tools, methods, processes and project plan for assessments and research. | - |
| 6 | Conduct survey and interviews with participating digital forensic practitioners, managers, and investigators. | ✓ |
| 7 | Analyse feedback and findings. | - |
| 8 | Perform Current State Assessment, and SWOT analysis of current offerings, benefits and challenges. | ✓ |
| 9 | Design DF-C²M², revised assessment tools, workflows, knowledge base goals and criteria. | - |
| 10 | Conduct workshops and seminar on draft DF-C²M² for review, and solicit feedback and areas for improvement from interviewees. | ✓ |
| 11 | Conduct an audit/assessment of an existing ISO 17025 digital forensic accredited lab against DF-C²M² requirements. Discuss and review findings with participating lab. | ✓ |
| 12 | Plan and implement updates to the accredited lab to bring it in-line with DF-C²M² requirements. | ✓ |
| 13 | Solicit evaluation on the model from participating labs/practitioners | ✓ |
| 14 | Incorporate changes/updates as may be required into DF-C²M². | - |

Participatory design was used at several key stages throughout this research as highlighted above. Key areas where practitioners were most influential were in assessing the DF-C²M² Body of Knowledge, Assessment Tool, Skills Assessment/Needs and Service Catalogue.

Practitioner from participating labs were involved in reviewing the DF-C²M² Model and Body of Knowledge during the workshops, and assessments, with more senior practitioners involved in detailed reviews and discussions around the practicalities and 'nice to have' aspects that they wished could be included. Certain decisions made with regards to the scope and components within the model were based on the researcher's experience/assumptions, whilst other were made based on a consensus opinion amongst practitioners from participating labs. In all such instances the justification or rationale behind certain decisions is indicated.

Key areas where participatory design input has significant effect on the research elements:

1. The need to include a means of measuring customer's satisfaction within a given lab over time.
2. Inclusion of certain value-add services within the Service Catalogue, and revision of Service Descriptions, and limitations.
3. Inclusion of ASCLD-LAB supplemental requirements within the Assessment Tool specifically related to validation of tools/methods, and proficiency testing.
4. Determining Service Catalogue prerequisite services/tools and processes prior to delivery of a service.
5. Determining annual management reporting requirements as per ISO 17025 requirements.
6. Determining challenges as they affected managers, examiners, and junior personnel.
7. General feedback on usability and content of the Body of Knowledge.
8. Feedback on the usefulness, viability and roadmap of the model.

## 4.3 PARTICIPANT EVALUATIONS OF THE MODEL

Participants involved in the detailed model and body of knowledge review participated in a written evaluation based on an evaluation form created following the labs assessments. The evaluations were anonymous, but certain demographic data was gathered as per the evaluation form cover page in Appendix A. Appendix C contains extracts of the online survey questions and their results. Appendix D contains extracts of some of the interviews held with practitioners during the practitioner interviews.

During reviews of the model and the body of knowledge key challenges raised by the practitioners were used to assess how best to address these, and if they should be included within the model. Certain aspects of the model including the body of knowledge (processes and workflows), assessment criteria and service catalogue inclusions were debated at length, and updates were incorporated within the key elements to reflect the consensus view for each of these elements. Practitioner feedback to these questions assisted in reviewing the model and its approach.

Overall participants were asked 55 questions based on the workshops and reviews and the findings. Participant feedback obtained via the workshops, assessments, interviews and the formal evaluation form were used to revise certain elements of the model, and provided validation of the key design components.

## 4.4 SUMMARY

Input from practitioners was a vital part of this research. Practitioners were involved and key stages and provided valuable input, suggestions and validation of the model and its planned approach.

Key aspects of design process where practitioners were involved:

1. Online survey
2. Face-to-face interviews
3. Conduct workshops and seminar on draft DF-C$^2$M$^2$ for review, and solicit feedback and areas for improvement from interviewees
4. Conduct an audit/assessment of two existing digital forensic accredited labs against DF-C$^2$M$^2$ requirements.
5. Discuss and review findings with participating lab.
6. Solicit feedback from participating labs.

# CHAPTER 5: DF-C$^2$M$^2$ - THE DIGITAL FORENSICS - COMPREHENSIVE CAPABILITY MATURITY MODEL

## 5.0 INTRODUCTION

This chapter describes the processes used for the design of the Digital Forensics – Comprehensive Capability Maturity Model (DF-C$^2$M$^2$). It includes the justifications for inclusions and additional critical factors identified during the problem identification and initial assessment phase of the research.

Specifically, it will present how previously identified gaps affecting People, Processes, and Tools contributed towards the creation of the DF-C$^2$M$^2$. It will examine each core section/module within the DF-C$^2$M$^2$ and describe how it was designed and the key elements contained within.

Additionally, this chapter introduces the assessment tools, methods, and criteria designed and used for this research. It examines the criteria employed to evaluate the present standards, based on the research questions defined in Section 1.4.2.

### 5.1 ADDRESSING RESEARCH QUESTIONS

In order to achieve the research objective, a set of methods and tools to help assess and address the main research questions outlined in Section 1.4.2 needed to be defined and created. Involving practitioners in the review and feedback of the model was a key aspect of this research, as user participation or participatory design (Sanders, 2008) is a proven method for tackling complex user problems and as a means of gaining active user ‘citizenship’/involvement in projects of a wider community interest (Murphy & Hands, 2012).

Designer Amos Winter emphasised that the key to successful design was to involve the intended user(s) in the design and solution development process, soliciting their input on the issues, but also, rather uniquely; on how they think the solution can best be achieved (Winter, 2012).

Winter's philosophy extended the basic principles of Participatory Design (Sanders, 2008) and was based on the principles of collective or Co-design. Throughout this research, practitioner feedback was sourced as to the practicality and suitability of elements, whether certain baseline assumptions made were reasonable, or whether they should be adjusted and why, and how certain tasks could be better implemented/designed or achieved.

This consultative approach to reviewing and improving upon elements within the model allowed for a more inclusive and engaging experience for participants as theorised by Murphy and Hands (Murphy & Hands, 2012).These dynamic feedback and interactions allowed for refinements of key elements, and provided a soundboard for validating ideas and proposed solutions.

The majority of digital forensic models developed to date, provide no indication of involvement or inputs from other practitioners other than perhaps drawing from the experience of the author(s). With DF-C$^2$M, bearing Sanders Participatory design philosophy (Sanders, 2008) in mind, a key design goal was to follow an iterative, consultative, and audit-based approach to conducting the research using a series of structured interviews, assessments, workshops, and reviews of related standards policies, procedures, and available literature – soliciting practitioner input on challenges and possible solutions (needs analysis).  Input from over 70 experienced digital forensic practitioners and managers on how best to address certain issues and on how to improve on existing systems and processes was key to helping make DF-C$^2$M$^2$ more holistic, and fundamental in helping to define what an ideal Body of Knowledge should contain and what key areas the model should address.

Additionally, in keeping with Kelvin's philosophy that the ability to measure is key to being able to improve upon a process (Thompson, 1910), the DF-C$^2$M$^2$ assessment tools were designed to provide both qualitative and quantitative data for detailed capability assessments, planning, and future benchmarking purposes.

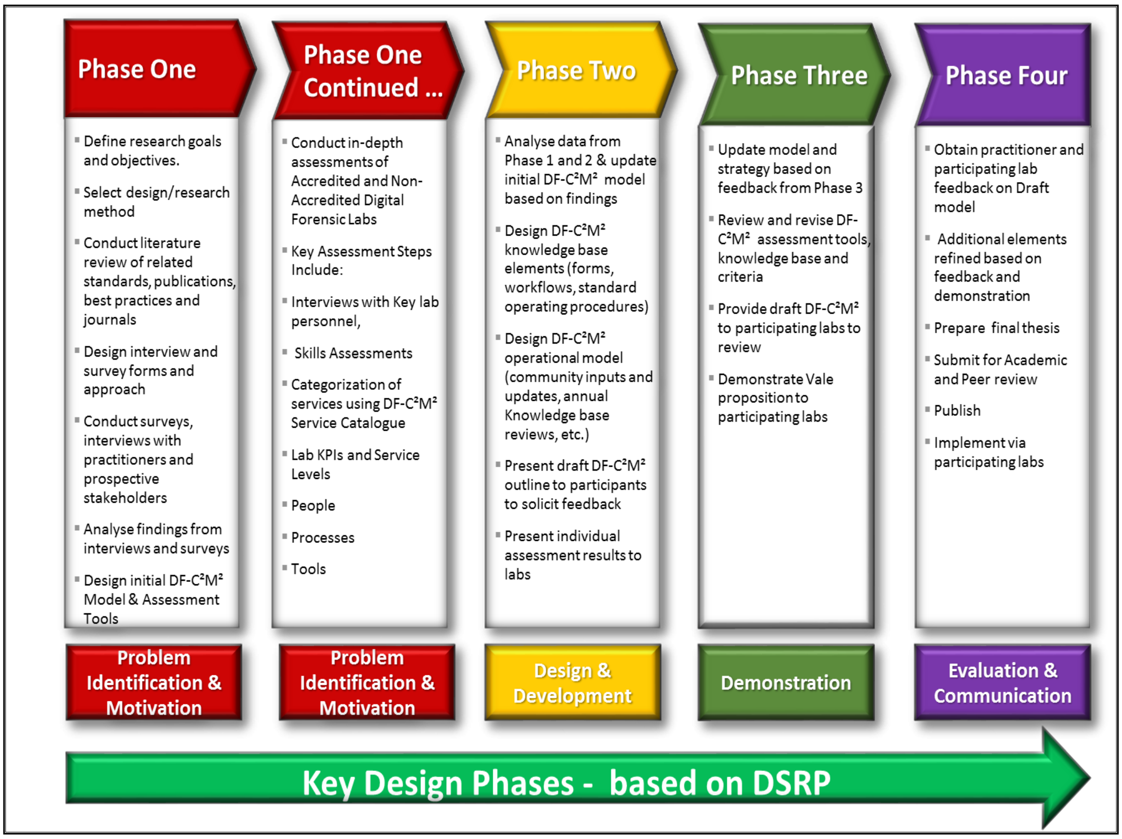
The first step in conducting the research was to select the research method best suited to designing models related to technology. To that end, the Design Science Research Process (DSRP) (Peffers et al., 2006) was selected as the framework for the research method and approach.

### 5.1.1 Key Phases of Research Using the DSRP

The key research activities performed as defined within the DSRP were:

1. Problem Identification and Motivation,
2. Design and Development
3. Demonstration (Proof of Concept)
4. Evaluation and Communication

Figure 2 provides an outline of the key stages performed during this research mapped to the DSRP model.



**Phase One**

- Define research goals and objectives.
- Select design/research method
- Conduct literature review of related standards, publications, best practices and journals
- Design interview and survey forms and approach
- Conduct surveys, interviews with practitioners and prospective stakeholders
- Analyse findings from interviews and surveys
- Design initial DF-C²M² Model & Assessment Tools

Problem Identification & Motivation

**Phase One Continued ...**

- Conduct in-depth assessments of Accredited and Non-Accredited Digital Forensic Labs
- Key Assessment Steps Include:
- Interviews with Key lab personnel,
- Skills Assessments
- Categorization of services using DF-C²M² Service Catalogue
- Lab KPIs and Service Levels
- People
- Processes
- Tools

Problem Identification & Motivation

**Phase Two**

- Analyse data from Phase 1 and 2 & update initial DF-C²M² model based on findings
- Design DF-C²M² knowledge base elements (forms, workflows, standard operating procedures)
- Design DF-C²M² operational model (community inputs and updates, annual Knowledge base reviews, etc.)
- Present draft DF-C²M² outline to participants to solicit feedback
- Present individual assessment results to labs

Design & Development

**Phase Three**

- Update model and strategy based on feedback from Phase 3
- Review and revise DF-C²M² assessment tools, knowledge base and criteria
- Provide draft DF-C²M² to participating labs to review
- Demonstrate Vale proposition to participating labs

Demonstration

**Phase Four**

- Obtain practitioner and participating lab feedback on Draft model
- Additional elements refined based on feedback and demonstration
- Prepare final thesis
- Submit for Academic and Peer review
- Publish
- Implement via participating labs

Evaluation & Communication

Key Design Phases - based on DSRP

**Figure 2: DF-C²M² key research steps**

Each stage of the DSRP enabled the research to apply a systematic approach to the DF-C²M² design from initial problem identification to requirements specification, and from a detailed design development through test implementation and final evaluation.

The use of the DSRP enabled a multitude of design transformations, from determining the requirements specification for creating a high-level design specification, from what was required, to how it best should be created, and from solution specification to detailed design and from design to product realisation and evaluation.

Various tools used for this research and assessments were designed or created as a means of gathering data, analysing data, and using those results for planning, assessments, and evaluations.

## 5.2 DF-C$^2$M$^2$ DESIGN CONSIDERATIONS

Several issues within existing digital forensics models and frameworks were identified in Chapter 2. Gaps within the prevailing digital forensics best practices and applied standards provide a unique opportunity for improvement to design a new digital forensics models to address these shortcomings, whilst introducing capability maturity as a key organisational goal in digital forensics. This concept was supported by the majority of practitioners that participated in the workshops and model evaluation.

Analysis of the various gaps and problems identified in Chapter 2 in addition to participant feedback on challenges and issues assisted in helping to identify key areas for improvement that; would enhance the present standards and best practices for People, Processes, and Tools aspects of a digital forensics organisation and enhance its organisational capability maturity.

The DF-C$^2$M$^2$’s consultative research and participatory design approach provides inclusive view of what needs to done, how it should be done, and how to integrate the multitude of requirements into a simple yet comprehensive digital forensics framework that incorporates standards, planning, and assessment tools – all view a focus on capability maturity across all elements as they relate to People, Processes, and Tools. This approach proved to be essential during the Problem Identification, Motivation, Evaluation, and Communications phases of this research, and as inputs into the Total Quality Management Analysis of challenges previously highlighted in Chapter 1.

## 5.3 TOTAL QUALITY MANAGEMENT (TQM) APPROACH TO ASSESSING THE DF-C$^2$M$^2$ KEY ELEMENTS

The research process focussed on the three key organisational components (People, Processes, and Tools) that contribute towards organisational Capability Maturity. The three key elements were expanded upon to detail sub-components, and the inter-relationship between each key element was identified.

In order to be better define the various influence factors that could affect each of the domains, and to better define the challenges faced by digital forensic laboratories, a basic Total Quality Management (TQM) (American Society for Quality, 2012) analysis was performed, and the resulting workflow Digital Forensics Organisation Challenges – TQM Analysis is depicted in Figure 3. Practitioner input was key in determining and narrowing down the list of key element and challenges in the TQM Analysis in Figure 3.

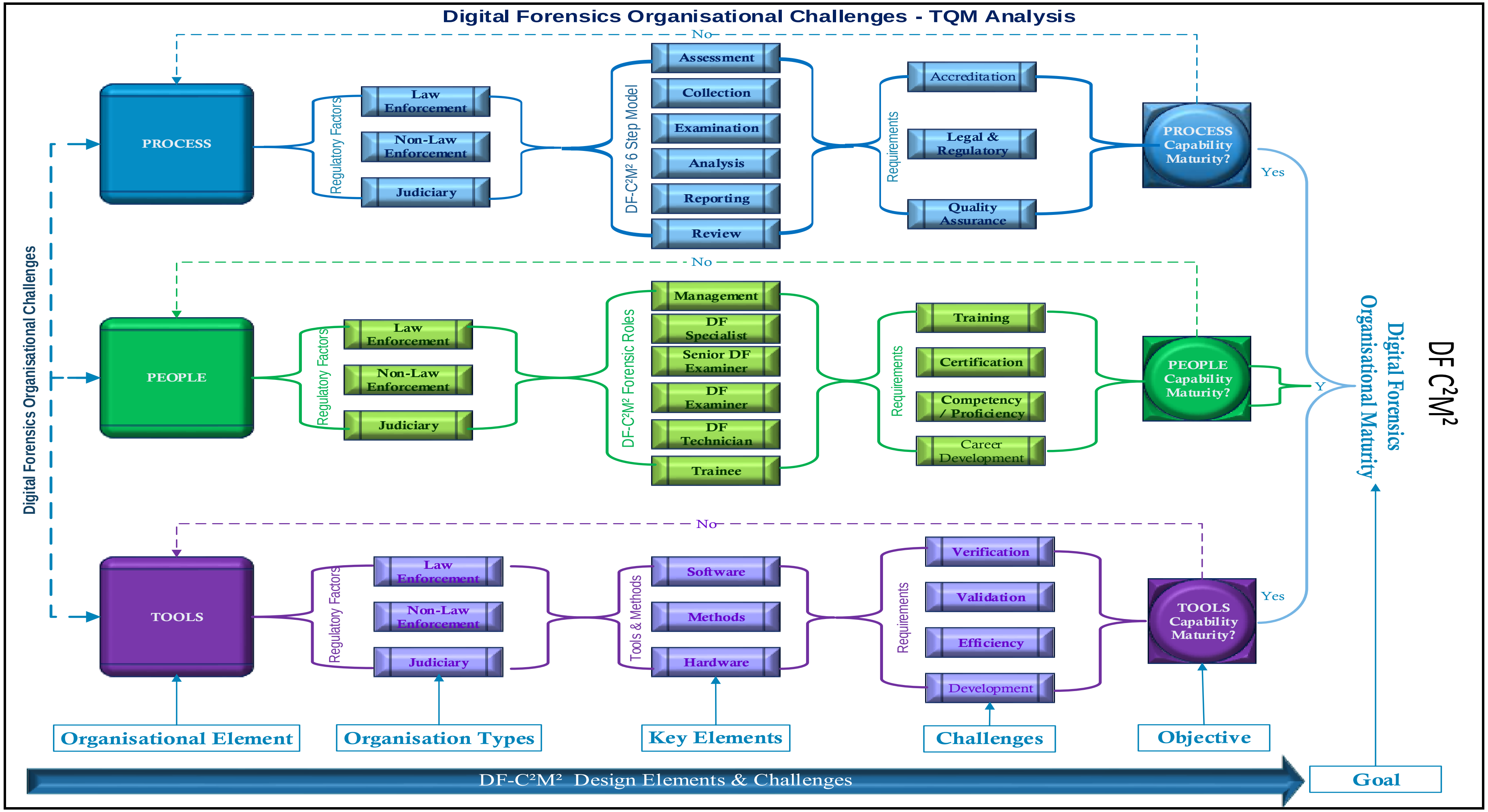


Figure 3: DF-C²M² domains and capability maturity key elements, challenges and objectives – TQM analysis

For each key element (People, Process and Tools) depicted above, the organisational type and what prevailing regulatory requirements may apply of affect them were considered (shown as the Organization Type).

The key sub-element of each core domain (People, Process and Tools) were identified (shown as Key Elements).

Next the constraints that the above sub-elements created were identified and assessed. For each sub-element, the key challenges and constraints were categorised (shown as Challenges). These constraints highlight essential requirements that pose major challenges and overheads (time, manpower and additional processes that must be performed) to accredited digital forensic laboratories.

Finally, the objective for each key element was defined for example within the Tools domain; Tool Capability Maturity was defined as the ultimate objective (Objective). Collectively the objectives of each key domain People, Process and Tools would ultimately contribute towards the final goal of Digital Forensics Organisational Capability Maturity (shown as Goal). This iterative analysis process was then repeated for the remaining key elements People and Process.

Thus, the TQM analysis of each key element presented a clear view of key focus areas that need to be assessed, and then later addressed via tools, knowledge base, and design of the DF-C$^2$M$^2$ framework.

The TQM analysis was applied to help form a critical part of the DSRP Problem Identification and Motivation stage of the research, and played a vital role in helping to plan, design and structure the range of interview questionnaires, assessment criteria and assessment tools. TQM assisted in helping to better evaluate the current ‘State of the Art’ of Digital Forensics Capability Maturity, and as the template upon which the various Digital Forensic models and framework discussed in Chapter 2 were assessed and evaluated.

## 5.4 DF-C$^2$M$^2$ PROCESS DOMAIN

### TQM analysis of the DF-C$^2$M$^2$ process domain challenges example

As stated in Chapter 1, addressing technical issues (tools) in digital forensic models without addressing non-technical issues related to other key domains such as Processes, including Process capability maturity, seems to be a common pitfall of many of the digital forensic models and frameworks assessed to date:

1. For the Process domain, for example, the organisational type and what prevailing regulatory requirements may apply to affect them were considered (shown as the Organisation Type in Figure 3).

   Three organisation types were identified (Law Enforcement, Non-Law Enforcement, and Judiciary was requested or inclusion during practitioner workshops). It was assumed that each organisation type would have different requirements regarding the processes used, levels of accountability, and audit requirements depending on the types of cases they may be required to process (Civil, Criminal, Internal Policy violations, etc.).

   Additionally, any levels of compliance with prevailing internal or external regulatory requirements would vary from one organisation type to another. Such requirements would ultimately affect how the organisation works and whether or not it is compelled to follow existing quality management and digital forensics standards in addition to trying to achieve organisational capability maturity.

2. The key Process elements were identified (shown as Key Elements in the TQM analysis in Figure 3). The key process elements of the Process Domain were identified and used as the basis for process requirements analysis, and as the basis for the creation of various process workflows within the DF-C$^2$M$^2$.

3. Next, the constraints (shown as Challenges in Figure 4) that the above sub-elements created were identified and assessed. For the Process sub-elements, the key Challenges and constraints previously identified in Chapter 1 were categorised as:

i). **Accreditation:** for an organisation wishing to achieve or maintain ISO 17025/ASCLD-LAB accreditation: The consensus opinion amongst participants was that maintaining accreditation requirements across a wide range of complex processes, and being able to effectively monitor and measure compliance with these processes across a large number of cases, proved to be one of the most taxing challenges faced by lab management.

- The result was a significant overhead in process controls that resulted in the creation of additional steps, documentation, and forms required for each process, case reviews, administrative and technical audits, and measurement of KPIs.

ii). **Legal and Regulatory:** Compliance with legal and regulatory requirements was often identified as an ongoing key challenge by the practitioners interviewed.

iii). **Quality Assurance/Managerial Review and Oversight:** Regardless of whether an organisation had or planned to gain accreditation for standards such as ISO 17025, all organisations were concerned about effective quality management and managerial oversight on results and processes used to obtain such results. Quality management was therefore factored into all aspects of the assessments and design of the DF-$C^2M^2$.

iiii). **Forensic Readiness** was also identified as a key managerial concern by senior practitioners, and this therefore also contributed towards a significant part of the assessment and planning requirements.

Finally, the objective for each key element was defined, i.e. Process Capability Maturity was defined as the ultimate objective (Objective) of the Process domain. Using this approach, several forms of CMM were incorporated into the model from CMM to P-CMM, unlike previous models and frameworks to date. Ultimately, Process Capability Maturity would contribute towards the final goal of digital forensics organisational capability maturity and help to address the major challenges related to accreditation and regulatory requirements.

The DF-C$^2$M$^2$ Process domain enables practitioners to address the most pressing process-related challenges while providing a set of tools to assist with assessment and enabling improvements across the scope of the processes.

### 5.4.1 DF-C$^2$M$^2$ Six Steps Forensic Process Model

An assessment of the participating labs showed that examination request typically went through six distinct stages of processing within the labs. These six distinct stages identified were analysed and translated into a simplified model that were viewed by participants to be best suited to digital forensic laboratories and digital forensic investigations. In contrast, a review of existing digital forensic and incident response models found that these typically involved 4, 8, or 12 steps, and were viewed by the majority of participants as being either too broad and generic, or too technical process-focussed, or too information security/security incident response focussed rather than digital forensics lab specific The resulting six steps model helped to identify and document the various stages of an examination, and later assisted in helping define the required skills to perform the various distinct tasks required at each stage. Decisions as to what include within the model drawn from initial experience on the process of following an artefact from initial planning for a seizure through to reporting and review. These elements were then validated based on findings such as interviews, assessments, and participant review of the model many of whom viewed it as a training tool for new personnel to explain basic lab examination processes from ‘A to Z’.

The DF-C$^2$M$^2$ Six Steps Forensic Process Model (see Figure 4) assisted in identifying key process elements related to digital forensic examinations, their input sources, and specific steps involved at each stage of processing.

The six key process elements as depicted in the DF-C²M² Six Steps Forensic Process Model are:

- **Assessment -** areas of concern identified included process-related case acceptance, investigative planning strategy, and resource allocation.
- **Collection –** includes processes and best practices to identify, document, collect, and maintain chain of custody, and preserve digital forensic evidence. This process element was identified as an ongoing iterative task to be included in all subsequent tasks hereafter. Collection includes documenting the said evidence, and forensic imaging or extraction of the exhibits submitted for examination
- **Examination –** included processing steps, extraction of data and inclusions of best practice methods and process elements required for evidential and ISO 17025 purposes such as technical notes, documentation of actions taken, and verification of tools as the start of each examination.
- **Analysis –** includes best practices and guidelines required to ensure impartial, complete, and sound evidentiary analysis of results used to produce any derivative evidence.
- **Reporting -** includes reporting guidelines (determined by Organisation Type), structure, format, and rules governing how to present the evidence in an unambiguous, impartial, and non-technical manner.
- **Review –** includes quality management elements that may include lessons learnt, performance statistics generation, and technical and administrative peer reviews.

The DF-C²M² Six Steps Digital Forensic model enables planned/future standards to be mapped into the Six Step model, which largely already covers the majority of the requirements of the planned future standards related to digital forensics. For example, the requirements for ISO 27037 for digital evidence handling and preservation requirements could easily be incorporate into the Collection, Examination, Analysis and reporting stages of the six-step model. Likewise, ISO 27042 for analysis and interpretation of digital evidence results could be integrated as requirements into the Analysis stage of eth six step model if so required.

#### 5.4.1.1 Summary notes regarding the Six Steps Model:

**Level One:** Identifies the key, distinct stages of Assessment, Collection, Examination, Analysis, Reporting, and Review.

**Level Two:** Identifies inputs, decision criteria/factors, and specific processes such as Incident Facts and related events.

**Level Three – depicted at the bottom of the Six Steps model illustration:** Identifies what is being worked on during each of the six steps, and ties in with the six steps identified in Level One, for example:

1. Assessment of case requirements,
2. Collection of media,
3. Examination of data,
4. Analysis of Information,
5. Reporting on evidence, and
6. Review of examination process and results.

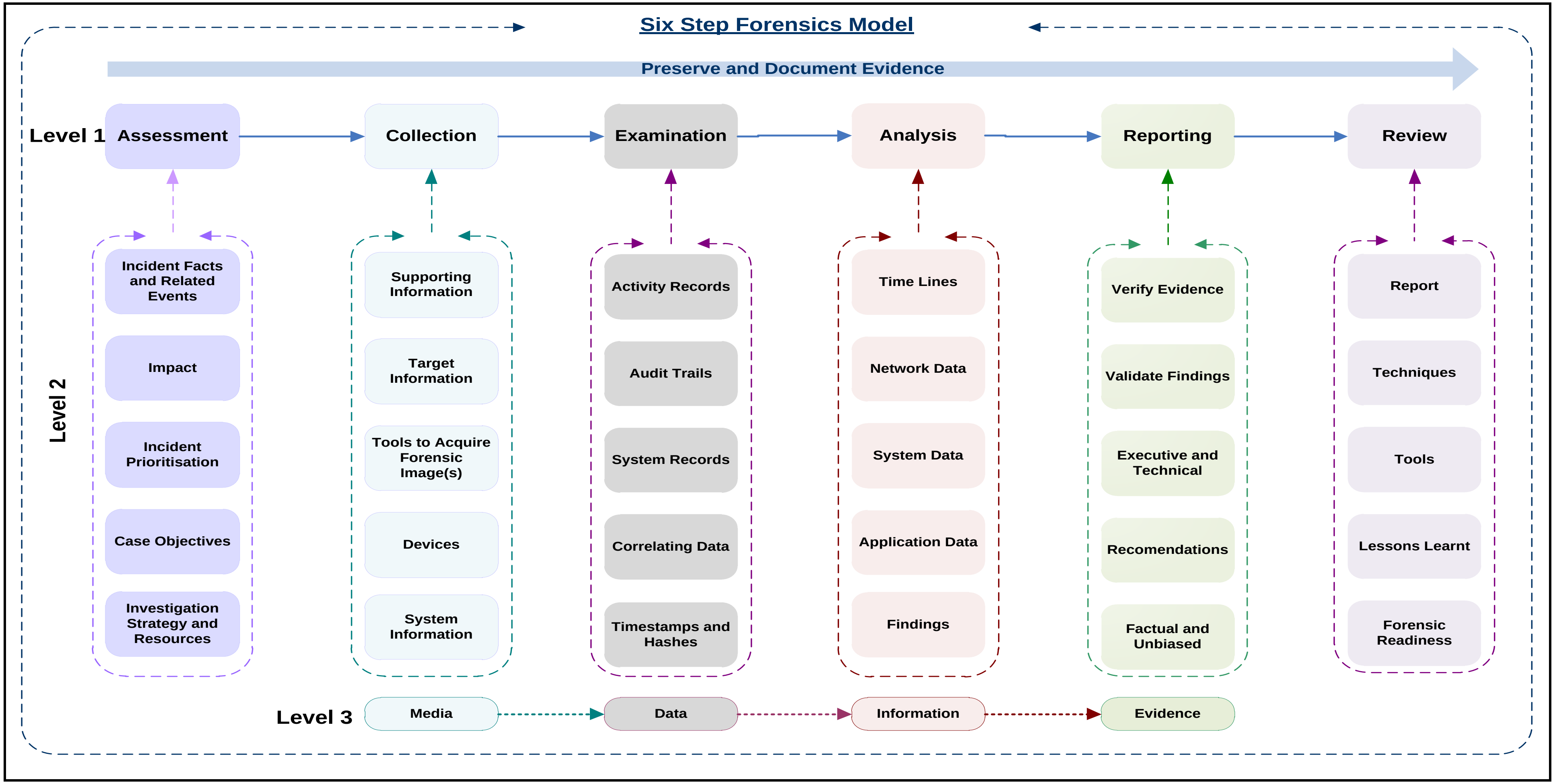


Figure 4: Six steps digital forensic lifecycle model

### 5.4.1.1 Incorporating and Mapping Standards into the Six Steps Model

Presently, the task of trying to map existing with proposed ISO-related standards (and overlapping functions, excluding ISO 17025) is quite complex, as depicted in the ISO mapping shown in Figure 5:

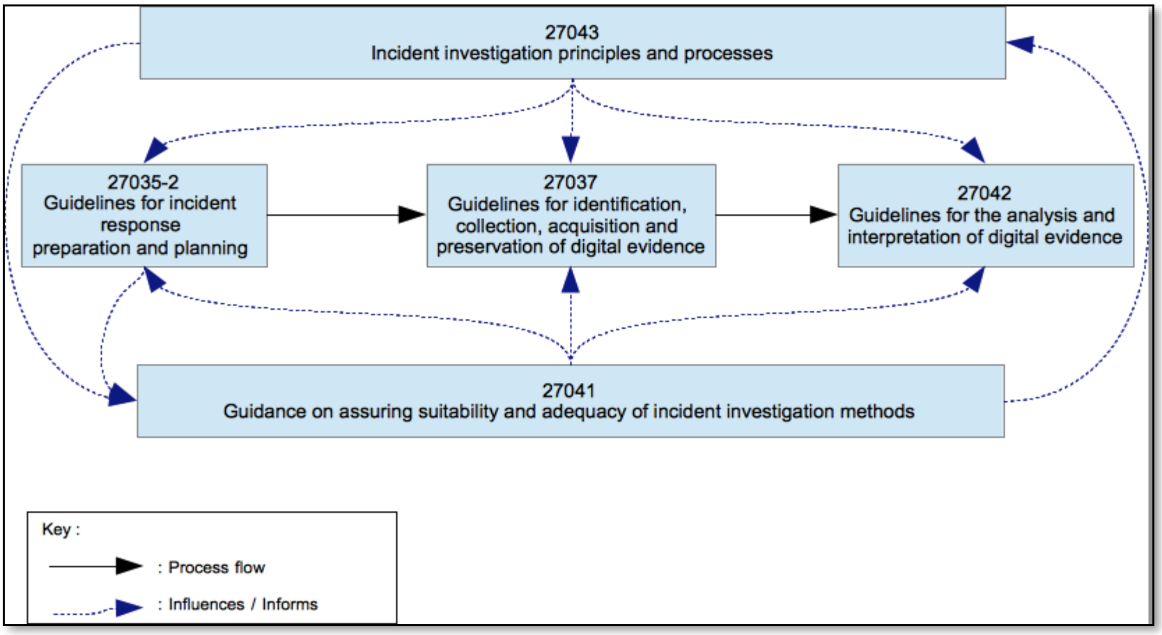
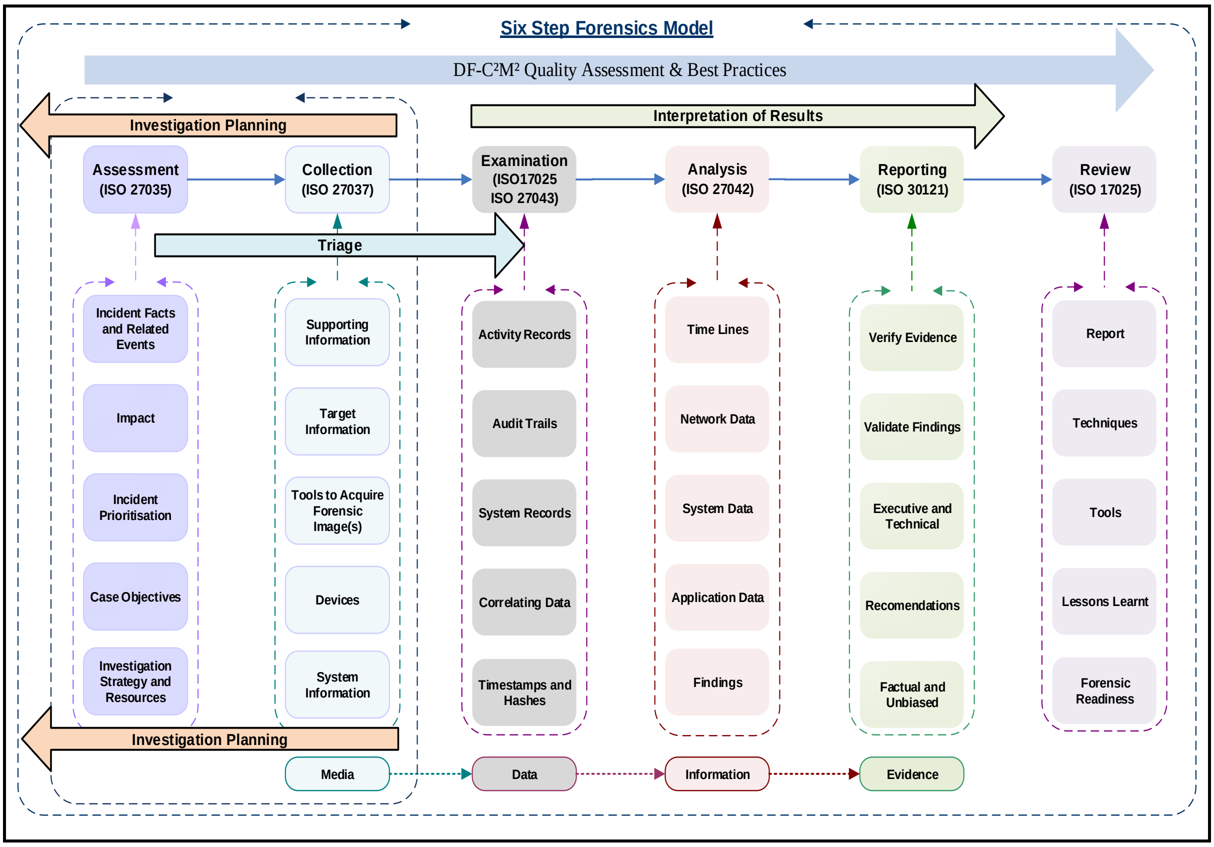

27043
Incident investigation principles and processes
27035-2
Guidelines for incident response preparation and planning
27037
Guidelines for identification, collection, acquisition and preservation of digital evidence
27042
Guidelines for the analysis and interpretation of digital evidence
27041
Guidance on assuring suitability and adequacy of incident investigation methods
Key :
: Process flow
: Influences / Informs

Figure 5: ISO 27000 series planned inter-relationships

(Source: International Standards Organisation)

The DF-C²M² Six Steps Model, by design, already addresses the majority of the requirements in the draft versions of these proposed standards. A mapping of the present and planned ISO standards within the DF-C²M² Six Steps Model is shown in Figure 6, with planned/proposed ISO standards shown in parentheses.

The DF-C²M² Six Steps model provides a structured digital forensic specific process model that identifies the key phases during an examination, the inputs and expected outputs allowing for streamlining of processes across digital forensics labs, and to provide a common framework upon which examination can be performed, as well as to help to address the issues previously identified in Chapter 1. The DF-C²M² Six Steps Model serves as a key source of inputs used as a guide for helping to define and create the various criteria required for the delivery of each service within the DF-C²M² Service Catalogue.



### Figure 6: A mapping of planned and future ISO standards within the DF-C²M six steps process model

To help address the issue of lack of planning and assessment tools as identified in Chapter 1, for each sub-element listed above, a bespoke set of assessment and planning criteria were created within the DF-C²M² Planning and Assessment Tool. The process elements identified included both technical and non-technical processes that would need to be sufficiently documented to enable an organisation to maintain a standard unified method of processing examinations, and to enable compliance with both ISO 17025 and Process Capability Maturity.

Validation of the mapping of ISO standards was performed based on a review of each standard and draft outlines of planned standards. Note that several of the stated ISO standards were released after the lab assessments conducted and therefore the mapping of these standards was not reviewed nor validated as part of the lab assessments and DF-C²M² evaluation, Independent detailed validation of these mappings may still be required to identify any possible oversights. As of the time of this research this mapping to ISO standards referenced above was complete and validated by the author, based on ISO published list of available and planned (draft) standards.

To help address issues related to the lack of uniformity in the way in which tasks are performed, a related digital forensic Case Progress Checklist was created as part of the knowledge base as a guide for digital forensic examiners to ensure that all examinations are performed uniformly with the same key steps, across the evidence collection, processing and analysis through to reporting stage of the six-step model. The Case Progress Checklist is part of the Body of Knowledge process domain.

Additional tools for each of the Six Steps areas were created to help address the gaps within the existing standards and best practices and to help achieve process uniformity across digital forensic labs.

## 5.5 DF-C$^2$M$^2$ PLANNING AND ASSESSMENT USING THE DF-C$^2$M$^2$ SERVICE CATALOGUE

Planning is a key element of the DF-C$^2$M$^2$, including Quality Management and Capability Maturity. Quality planning can be defined as a ‘Systematic process that translates quality policy into measurable objectives and requirements, and lays down a sequence of steps for realizing them within a specified timeframe’ (Business Dictionary, n.d.).

A key element within the scope of the Process domain is organisational planning. However, it was discovered that none of the existing digital forensic models evaluated in Chapter 2 adequately addressed organisational planning challenges within their scope – a fatal oversight.

As such, a key assessment, planning, and management support tool referred to as the *DF-C$^2$M$^2$ Service Catalogue* was created to help identify all services that a digital forensics laboratory may be required to provide and to help identify their inter-relationships and dependencies. More importantly, the Service Catalogue was designed to enable organisations to effectively plan and assess their People, Processes, and Tools requirements for the successful implementation and delivery of each service.

In helping organisations to better evaluate requirements versus benefits aspects for the delivery of each service, the Service Catalogue was designed to also factor

Complexity versus Impact analysis rating for each service. The Service Catalogue would therefore enable both the assessors and laboratory management to determine if they have the required People, Processes, and Tools elements prior to launching a new service, and to help identify any known limitations of each service.

Generally accepted best practice principles, and standards such as Information Technology Infrastructure Library (ITIL) standard (Information Technology Infrastructure Library, 2012), ISO 17025, and APCO principles are used in the delivery of these services. The ITIL guidelines suggest that a detailed catalogue of proposed services must be maintained and that the catalogue must be readily available to those who are approved to access it. The DF-C²M² knowledge base offers an extensive portfolio (template) of commonly requested pre-defined services to eligible authorised departments (customers).

The DF-C²M² Service Catalogue serves as a central repository of pertinent information planning information on each of the services. Whereas customers may use the catalogue to obtain an accurate view of available services, limitations, terms, and conditions and what benefits can be derived from it, the DF-C²M² will use the same information as a reference to enable labs to plan for delivery of these services, and develop its infrastructure, people, technology, and organisational architecture.

The DF-C²M² Service Catalogue contains sample Key Performance Indicators (KPIs) associated with each service and proposed Service Level Target (SLT) guidelines for each service.

Inclusion of service pre-requisites as they relate to the DF-C²M² key domains (Processes, People, and Tools) and input from the DF-C²M² assessment/readiness planning tool will assist labs in incorporating capability maturity and quality of service in the Service Catalogue, which will serve as one of the primary digital forensic lab planning and roadmap tools.

Using the DF-C²M² Service Catalogue, a lab's capability maturity can be assessed by:

- The number of services being delivered as a percentage of those recorded and managed within the Service Catalogue.
- The number of detected deviations between the services actually delivered and those described within the lab's Service Catalogue.

- Verification that the required skills, tools, processes, methods, and other prerequisite dependency services are in place for the effective delivery of each service.
- The general level of the customer's awareness and understanding of the services, any limitations, and terms and conditions of lab service.
- Lab's personal awareness of, and their proficiency in, the tools, methods, and processes for delivery of each service.
- Percentage increase in the completeness of the prerequisite components that support the services described in the Service Catalogue.
- Quality assurance feedback results from an individual lab's customers for example, did the service meet the expectations, were the results clear and concise, is there anything that could be done to improve the service, and overall how satisfied were they with the service from initial submission through to final completion.
- Technical accreditation, and proficiency and competency testing results of lab personnel involved in the delivery of each service.

### 5.5.1 DF-C$^2$M$^2$ Service Catalogue Categories of Service

A key issue discovered during this research was that most organisations had no structured method or process for planning and assessing the value/impact of current and future services offered to clients. Planning and delivery of services are organisational process concerns that affect, and are affected by, People, Processes, and Tools.

The idea for a Service Catalogue that lists services available and limitations was derived from a previous project, where as Director of a Police Station, the researcher had created a service catalogue was created for the public detailing services available to them and the requirements to use each service. For each the prerequisites for the delivery of each service were defined together with any applicable limitations are service level targets.

The DF-C$^2$M$^2$ Service Catalogue took the same concept to a much more detailed and granular level as a planning and readiness tool. The idea to categorise services based on lab units within a lab was based on the structure the researcher had previously created as part of a digital forensic lab project. Service Categories such as Live & Network Forensics and Digital Evidence Handling was based on input from practitioners involved in various aspects of the project. Cybercrime analysis was based on survey participant feedback.

The DF-C$^2$M$^2$ Service Catalogue was designed as a tool to assist with planning, evaluation, and delivery of digital forensic services, and as such, it is a key process planning and assessment tool within the DF-C$^2$M$^2$.

The Service Catalogue pertains to and affects the People, Processes, and Tools domains. It is referenced within all three domains as a key planning and benchmarking point of reference. Essentially, the Service Catalogue helps to define the unique requirements for each of the three domains based on services delivered and their related prerequisites, KPIs, and limitations.

Inclusion of a service within the DF-C$^2$M$^2$ Service Catalogue was based on five key influencers identified by workshop practitioners and the researcher and these included:

1. Customer feedback/changing business or legal needs
2. Trends (based on new devices, services, solutions, crimes)
3. Results of any research and development projects
4. Current global best practices
5. Organisational strategic plan/vision

Based on participant lab feedback on most commonly requested digital forensic services, and insight on current digital forensic trends, 37 services divided into six categories of services were initially identified within the DF-C$^2$M$^2$ Service Catalogue, these are:

1. Computer Forensics
2. Mobile Handset Forensics
3. Digital Audio and Video Forensics
4. Network and Live Forensics
5. Digital Evidence Tactical (and on-site) Support
6. Cyber Crime Investigation Support

The Service Catalogue lists the typical and most frequently requested digital forensic related services that a digital forensic laboratory may be asked to provide – known as Core Services. Core Services are essential, most commonly expected and requested services that the lab is expected to provide based on participant feedback. The catalogue also lists advanced/future services that may not be immediately required, but have been added to as Value-Add services i.e. not essential for the majority of examinations, but nice to have such as Advanced password recovery, static malware analysis, or perhaps examination of damaged mobile handsets via chip removal and analysis, etc.

For each service within the six distinct categories of services, the DF-C$^2$M$^2$ provides:

- Service objective and definition,
- Service context and dependencies,
- Tier of customers who can access the service,
- Status - Phase of the digital forensic lab development/roadmap when the service will be activated and made available to its customers,
- Sub-elements, prerequisites, and any limitations associated with the delivery of each service.
- Service Type: Core vs. Value-Added DF-C$^2$M$^2$ service rating for each service

These services listed within the Service Catalogue cover the majority of the general types of services a typical law enforcement digital forensic laboratory would be expected to provide. Table 8 is a sample extract taken from the DF-C$^2$M$^2$ Service Catalogue Planning Tool:

**High-Level Service Catalogue List of Computer Forensics (CF) Services (Planning & Assessment View):**

Table 8: Sample service catalogue service table summary ratings

| Category | Service Description | Dependency on Other Service(s) | Status | % | Core or Value Added | Impact Rating | Complexity Rating |
|---|---|---|---|---|---|---|---|
| **Ref:** | **Computer Forensics** | | | | | | |
| CF1 | Digital Data Extraction (Imaging) from Digital Computer Media | - | Fully Implemented | 100 | C | 10 | 5 |
| CF2 | Digital Forensic Examination & Analysis - Windows | CF1 | Fully Implemented | 100 | C | 9 | 7 |
| CF3 | Digital Forensic Examination & Analysis - Mac OS | CF1 | Fully Implemented | 100 | C | 9 | 8 |
| CF4 | Digital Forensic Examination & Analysis - Unix | CF1 | Partially Implemented | 70 | C | 9 | 8 |
| CF5 | Software Licensing Validation & Anti-Piracy | CF2 | Fully Implemented | 100 | V | 5 | 5 |
| CF6 | Decryption and Password Recovery | CF1, CCF2, CF3, CF4 | Partially Implemented | 50 | C | 6 | 9 |
| CF7 | Malware Verification and Behavioural Analysis | CF2, CF3 | Partially Implemented | 50 | C | 6 | 9 |
| CF8 | Digital Data Recovery from Damaged Computer Media | CF1 | Fully Implemented | 30 | V | 6 | 10 |
| CF9 | Computer Evidence Expert Witness Testimony | CF1, CF2, CF3, CF4 | Fully Implemented | 70 | C | 7 | 7 |
| CF10 | Digital Forensics On-Site Response and Seizure | CF1 | Fully Implemented | 60 | C | 8 | 7 |

For each service listed in Table 8, a detailed customer-focussed service description sheet is provided as per the example in Table 9:

### Table 9: Example DF-C²M² service catalogue – service description

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Reference** | **CF-1** | **Category** | **Computer Forensics** | | | | | |
| **Objective** | **Provide services for Digital Data Extraction from Digital Computer Media.** | | | | | | | |
| **Definition** | To provide data extraction and analysis services from a variety of digital computer media including: Computer Hard Drives (internal), USB (External) Hard Drives, USB Thumb Drives, CD ROM Media, DVD Media, Blue Ray Media, and Floppy Diskettes. | | | | | | | |
| **Service Context and Description** | | | | | | | | |
| • The Lab will, on request of eligible customers, provide forensically sound data extraction services from supported devices, including the analysis of any specific content that may be requested by investigators or the prosecutor.<br>• The LAB will also fulfil an advisory role with regards to best practice principles and methodologies that should be considered during the extraction of data from digital storage media as and when required.<br>• Engagement will be initiated by customers as a reactive 'Pull Service'. | | | | | | | | |
| **Available to:** | **Tier 1 (LEA)** | ✓ | **Tier 2 (Courts)** | ✓ | **Tier 3 (Govt.)** | ✓ | **Public** | - |
| **Service Status** | ✓ **Active** | **Not Active** | **Planned** | | | | | |
| **Associated Services and Functions** | | | | | | | | |
| • Device disassembly,<br>• Media Imaging,<br>• Data Recovery,<br>• Data Decryption Services | | | | | | | | |
| **Limitations of Service** | | | | | | | | |
| • Does not presently cover Magnetic Tape Media.<br>• Limited support for Hardware-based RAID Systems. | | | | | | | | |

The relevance of each service is initially determined based on the DF-C$^2$M$^2$ Service Catalogue usefulness i.e. Core vs, Value-Add, and the associated costs and prerequisites associated with implementing and delivering the service. During the participant workshops, following a review of the default DF-C$^2$M$^2$ Service Catalogues, the consensus amongst participants was that each service listed within the Service Catalogue was found to be adequately defined and labelled, and workshop participants identified the need for the catalogue to remain relevant and useful, that the catalogue should be reviewed at least annually by DF-C$^2$M$^2$ participating labs and the broader digital forensic community at large to determine:

1. Relevance to current and future lab operations.

2. Impact vs. Complexity (may affect decision-making related to 'insourcing' vs. outsourcing based on cost or complexity).

3. Number of service requests received, where this service was required and utilised or not available.

4. Envisioned future requests for such service, e.g. technology/device is soon to be obsolete, provision for new types of devices.

5. New or emerging standards and best practices such as the National Institute of Standards and Technology (NIST) May 2014 guidelines for Mobile Forensics (Rick, Sam, & Jansen, 2014).

### 5.5.2 Understanding the DF-C$^2$M$^2$ Service Catalogue - Impact vs. Complexity Ratings:

In order to help assess and determine the challenges related to implementing specific services, an Impact vs. Complexity matrix was incorporated into the Service Catalogue as a guide to assist lab managers.

The following summary describes the criteria to use when determining the Impact and Complexity values for each service within the DF-C$^2$M$^2$.

**Note:** These initial impact and complexity ratings were initially assigned labels of low, medium and high. In order to facilitate plotting the impact vs. complexity on a graph initial numeric values were assigned on a scale of 1 to 100 for complexity ratings, 1 to 10 for impact ratings. The method used for assigning these ratings has not been validated nor is it based on an existing method for determining impact vs complexity ratings.  Details on the ratings for impact, complexity and overall ratings per service is detailed further in this section. Practitioner feedback found the ratings system used to be acceptable, but most had preferred if it was based on any existing method for evaluating digital forensic services; of which there are none at present.

#### 5.5.2.1 DF-C$^2$M$^2$ Service Catalogue - Impact Ratings

Impact ratings are determined by the organisation, being assessed based on the nature of the organisation, and services they are legally and technically able to provide and the criticality of each service to the core business functions and customer requirements.

The DF-C$^2$M$^2$ Service Catalogue Planning Tool provides a recommended (default) Impact rating based on a consensus/average of the participants involved in the DF-C$^2$M$^2$ workshops and evaluation as part of the participatory method (Chapter 4) used throughout this research. These ratings are suggested rating and may be adjusted accordingly by each lab that utilises DF-C$^2$M$^2$ in future. It was also noted during the participant labs workshops by participants that some services may initially be thought of being Low Criticality, but may be vital to attaining/maintaining legal or accreditation status, and therefore this will be shown as mandatory. The initial Impact ratings are suggested ratings created by participant consensus, and would require broader peer review and inputs to help determine more accurate ratings for each. The default Impact (Criticality) ratings and Core vs. Value-Added service classifications are shown below:

- **Score: 9 to 10 = Mandatory Core Service:**

- Other services significantly dependent on availability of this service/provision of this service are a legal or regulatory requirement. No other services can be provided without availability of this service.

- **Score 7 to 8 = Critical Core Service:**

- Maximum business value derived from the provision of this service to customers and other services significantly dependent on availability of this service/provision of this service. Considered as a high priority core function/service.

- **Score 5 to 6 = Essential Core Service:**

- High business value derived from the provision of this service. Considered part of standard service offerings for a digital forensic lab. Other services may be dependent on the availability/provision of this service. Considered as a core function/service.

- **Score 3 to 4 = High Priority Value-Added Service:**

- High business value may be derived from the provision of this service. Some requests for this service have been received or it is envisaged that there will be an increase requested for such a service within the next 12 to 18 months. Not considered part of a digital forensic lab Core Service.

- **Score 2 = Low priority Value-Added Service:**

- Some business value may be derived from the provision of this service. Requests for this service are few, and it is not envisaged to increase significantly within the next 12 to 18 months. Not considered part of a digital forensic lab Core Service.

#### 5.5.2.2 DF-C²M² Service Catalogue - Complexity Ratings

The Complexity ratings used in the DF-C²M² Impact vs. Complexity tool were based on feedback from practitioners on the delivery of each service. For each of the complexity ratings a maximum weight or value was assigned based on the relative significance of each item in relationship to other complexity influencers. The combined score for a complexity calculation for a given service would be a maximum of 100 in total. In the absence of a complexity rating system for digital forensics examinations; these maximum weight values were apportioned based on the researcher's initial perceived importance of each of the complexity influencers listed below. The initial Complexity ratings are suggested ratings created by participant consensus, and would require broader peer review and inputs to help determine more accurate ratings for each. Likewise, as forensic technology and methods evolve, tasks that may initially have a high degree of complexity, may in future have a lower degree of complexity such as bypassing Pin Code protection on certain Android handsets, which today can be achieved using tools such as Cellbrite's UFED for PCs.

Complexity ratings consider three main planning aspects for the delivery of a service, namely:

1. Level of skills required to deliver the service. *Maximum Weight/Value: 30*
2. Tools (includes availability, cost of procuring and implementing the tools, and required prerequisites). *Maximum Weight/Value: 30*
3. Process (validated methods, procedures, and controls). *Maximum Weight/Value: 20*

Furthermore, two additional criteria that could affect the overall complexity of implementing/delivering the service include:

a. Total cost for implementation of the service (includes cost for tools, training, personnel, facilities, etc.). *Maximum Weight/Value: 10*

b. Ongoing cost for provision of the service on a case-by-case basis (e.g. the cost to recover 1 GB of data using Advanced Disk Repair services). *Maximum Weight/Value: 10*

The total DF-$C^2M^2$ Complexity rating is determined by the total score of all 5 criteria above divided by 10. For example, for Decryption and Password Recovery (CF6), the Complexity rating would be determined as follows:

| | |
|---|---|
| 1. Required Skills Level: | 25 |
| 2. Tools: | 40 |
| 3. Processes: | 15 |
| 4. Initial Cost | 10 |
| 5. Ongoing Cost: | 5 |

**Complexity Rating is: 95 divided by 10 = 9.5 out of 10**

The DF-C$^2$M$^2$ Complexity categories are listed below, with additional explanations for each category provided.

- Score 9 to 10 = Highly Advanced Complex Service,
- Score 7 to 8 = Advanced Complexity,
- Score 5 to 6 = Complex,
- Score 3 to 4 = Medium Level of Complexity,
- Score 1 to 2 = Low Complexity.

**The (Default) DF-C$^2$M$^2$ Complexity Ratings agreed by participants were:**

- **Score 9 to 10 = Highly, Advanced Complex Service:** Involves a very high degree of precision using complex methods, tools or systems and significant skills or expertise. Provision of this service poses very significant risk to the evidential integrity exhibits and the quality management system. (Mostly restricted to R&D efforts or extremely high-risk services). Delivery of this service should be reviewed on a case-by-case basis, and would require an approval for Procedure Deviation under ISO 17025/ASCLD-LAB requirements.
- **Score 7 to 8** = Advanced **Complexity**: Involves a high degree of precision using complex methods, tools or systems and advanced skills or expertise. A High-Risk service, which poses significant risk to the evidential integrity exhibits and the quality management system. Delivery of this service should be reviewed on a case-by-case basis, and would require an approval for Procedure Deviation under ISO 17025/ASCLD-LAB requirements.
- **Score 5 to 6** = **Complex:** Involves some degree of precision using relatively complex methods, tools or systems and skilled and experienced personnel. Provision of this service poses high, but acceptable risk to the evidential integrity exhibits and the quality management system. Risks still exist in the delivery of the service, but are manageable and should not affect the forensic integrity or quality management system.
- **Score 3 to 4** = **Moderate Level of Complexity:** Involves some degree of precision using well-established methods, tools or systems and reasonably skilled and experienced personnel. Provision of this service poses significant risk to the evidential integrity exhibits and the quality management system.

- **Score 1 to 2 = Low Complexity:** Involves low degree of precision using well-established methods, tools or systems and lower skilled personnel. Provision of this service poses minimal risk to the evidential integrity exhibits and the quality management system.

**Note:** Risks could affect the: degree of success of the service, forensic integrity, quality management standards, budget over-run and overall success and acceptability of the service.

Using the Impact vs. Complexity 'Magic Quadrant' in Figure 7, an organisation may choose to implement services that fall in the 'High-Impact, Low Complexity' and 'Low Impact, Low Complexity' services first, and then create a series of longer-term projects or plans to implement those services within the "High-Impact, High-Complexity" quadrant as per sample shown in Figure 7:

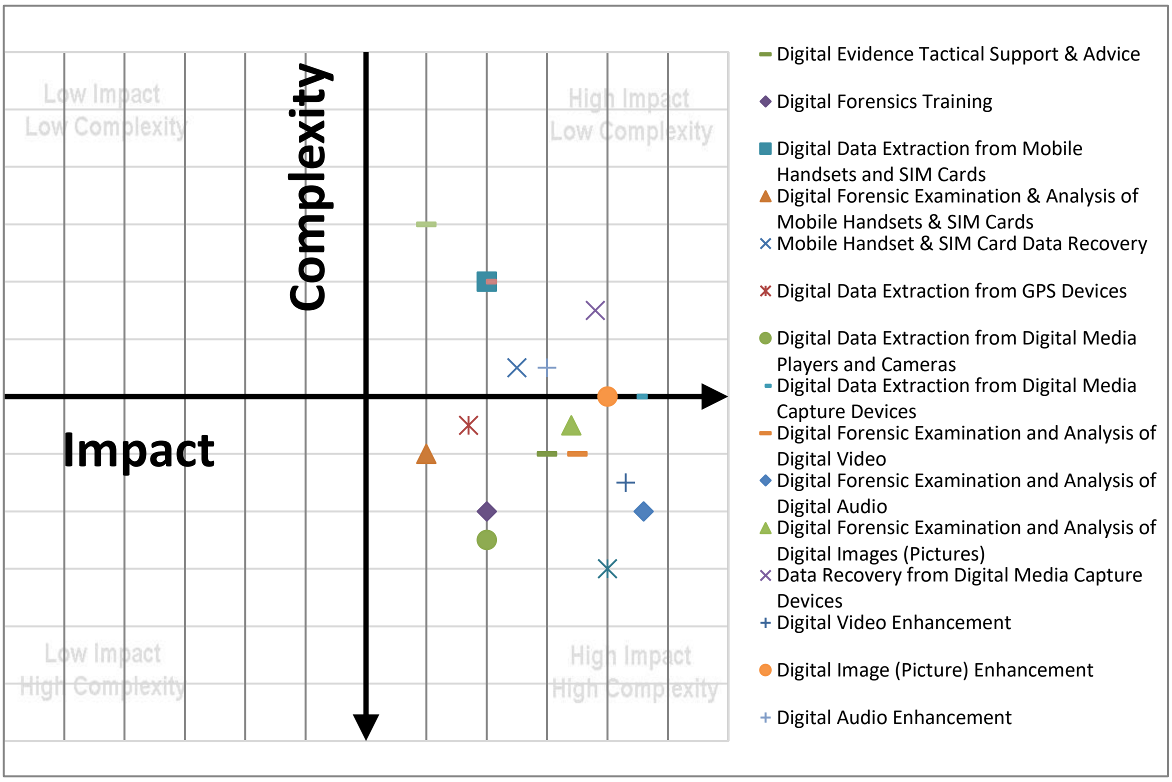


Figure 7: Sample DF-C$^2$M$^2$ impact vs. complexity planning 'Magic Quadrant'

The Impact vs Complexities used in the sample chart were based on participant group exercise consensus related impact vs complexity of each services for LAB #1 using a sub-set of the services defined within the Service Catalogue in figure 7.

#### 5.5.2.3 DF-C²M² Service Catalogues - Service Status and Process Maturity

For each service definition within the DF-C²M² Service Catalogue, the current status of the service needs to be assessed. DF-C²M² statuses for each service are defined based on the following guide (as used within the Service Catalogue):

- **Fully Implemented** – This service and all related offerings have been formally implemented, documented, and tested with no few or no limitations encountered. Provision of this service has reached a P-CMM level of maturity as demonstrated through the proficiency of the relevant examiners (subject matter experts). Service has been active for at least 6 months, and the service and all related support requirements (people, processes, tools) and relevance are reviewed every 6 to 12 months.
- **Partially Implemented** – The basic services related to this are active and operational. These services have been/are being tested and documented. Additional related support services, training, and testing are still required before the service can be considered fully operational. The lab has not yet reached a significant level of maturity and expertise (P-CMM) in the delivery of this service.
- **Planned but Not Implemented** – The need for this service has been identified as a business/legal requirement, and initial planning related to the tools, processes, and skills required for the successful implementation of this service has begun.
- **Not Planned Nor Required by the Nature of Business** – This service is not presently required, nor envisioned as a required service for the next 12 to 24 months.

### 5.5.3 Service Catalogue Planning Process - Priority Levels

To assist new labs in helping to decide which services to offer first, the Service Catalogue Priority Levels based on Impact vs. Complexity could be applied. As a basic rule of thumb, the both of labs were keener to implement 'High Impact, Low Complexity' services rather than 'Low-Impact, Low Complexity' services, etc.

The following lists the DF-C²M²'s four Planning priority levels (which cover all possible combined Impact and Complexity results) for any service (based on the DF-C²M² Impact vs Complexity service analysis) – grouped from least complex and most beneficial to more complex and least beneficial based on DF-C²M² Impact vs Complexity ratings):

- **Level 1:** High-Impact, Low Complexity
- **Level 2**: Low-Impact, Low Complexity
- **Level 3:** High-Impact, High Complexity
- **Level 4:** Low-Impact, High Complexity

Planning priorities are determined by each organisation, and the DF-C²M² assessment tools can be used to assess the status of current services and assist a new lab in planning which services should be implemented in which order based on the nature of their business and the Impact vs. Complexity analysis information presented within the DF-C²M².

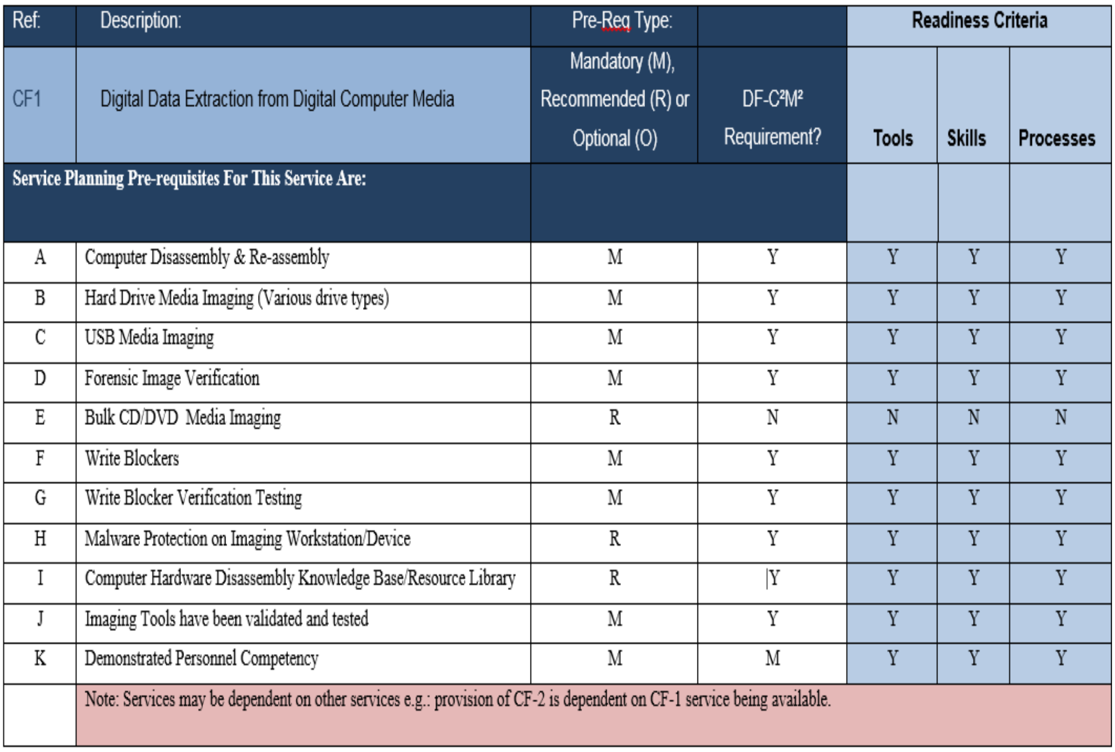
### 5.5.4. DF-C²M² Planning Process – Identifying Service Prerequisites

As identified during the practitioner workshops, practitioners from Lab #1 stated that delivery of each service may have certain dependencies identified within the Service Catalogue shown later in this document.  Additionally, each service will have a specific set of requirements for successful delivery of the service.

These prerequisite requirements enable planning for the delivery of each service, and a means to assess readiness prior to the delivery of each service or annually, as technology or organisational changes may affect the lab's future ability to deliver these services. The prerequisite requirements for each service look at the essential People, Tools, and Processes requirements (Readiness Criteria), and the Six Steps Model that must be in place prior to delivery of the service.

In the sample Service Catalogue in Table 10, the delivery of the service ‘Computer Forensics 1 (CF1)’ has no service dependencies; however, it has eight mandatory People, Processes, and Tools prerequisites (A to K), and three recommended requirements. Delivery of other computer forensics-related services may be dependent on the availability of this service.

Table 10: Sample service catalogue planning view for one service



| Ref: | Description: | Pre-Req Type: | | Readiness Criteria | | |
|---|---|---|---|---|---|---|
| CF1 | Digital Data Extraction from Digital Computer Media | Mandatory (M), Recommended (R) or Optional (O) | DF-C²M² Requirement? | Tools | Skills | Processes |
| Service Planning Pre-requisites For This Service Are: | | | | | | |
| A | Computer Disassembly & Re-assembly | M | Y | Y | Y | Y |
| B | Hard Drive Media Imaging (Various drive types) | M | Y | Y | Y | Y |
| C | USB Media Imaging | M | Y | Y | Y | Y |
| D | Forensic Image Verification | M | Y | Y | Y | Y |
| E | Bulk CD/DVD Media Imaging | R | N | N | N | N |
| F | Write Blockers | M | Y | Y | Y | Y |
| G | Write Blocker Verification Testing | M | Y | Y | Y | Y |
| H | Malware Protection on Imaging Workstation/Device | R | Y | Y | Y | Y |
| I | Computer Hardware Disassembly Knowledge Base/Resource Library | R | \|Y | Y | Y | Y |
| J | Imaging Tools have been validated and tested | M | Y | Y | Y | Y |
| K | Demonstrated Personnel Competency | M | M | Y | Y | Y |
| | Note: Services may be dependent on other services e.g.: provision of CF-2 is dependent on CF-1 service being available. | | | | | |

The Six Steps Model Level 1, 2, and 3 Processes, People, and Tools elements are factored into the Service Catalogue forensic services such as Computer Forensics (CF1). The DF-C²M² Service Catalogue provides a unique digital forensics planning tool for lab management, ensuring that they fully assess and understand the People, Processes, and Tools requirements for the successful delivery of each planned service as defined within the Six Steps Model.

## 5.6 DF-C²M² - PEOPLE DOMAIN

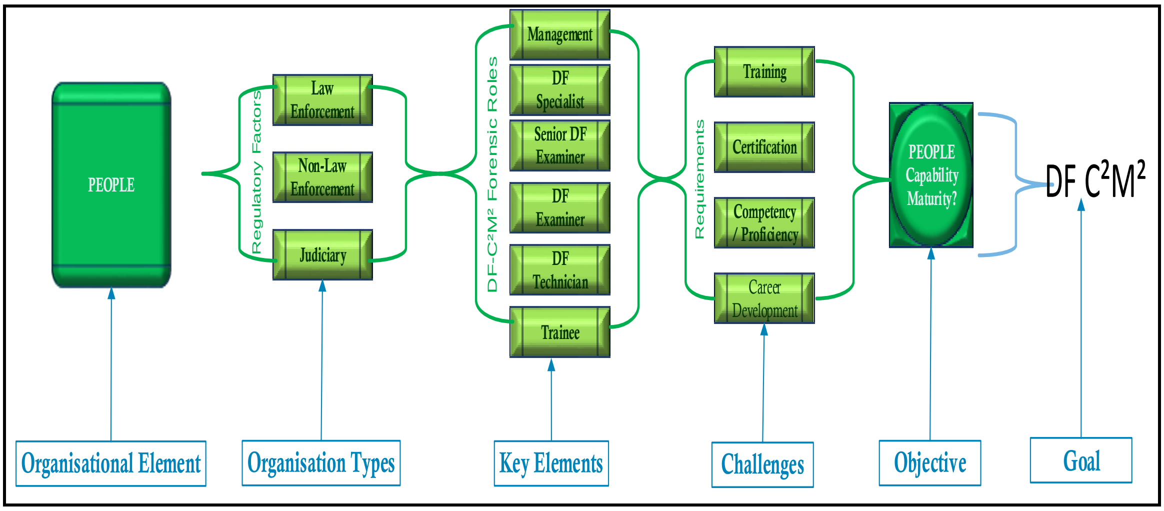


Figure 8: TQM analysis of DF-C²M² people domain challenges

It could be argued that efficient personnel lead to more efficient processes, and capability maturity of personnel contributes directly to the overall capability maturity of organisations. P-CMM was therefore used as the basis for the DF-C²M² People elements, with achieving digital forensic-specific P-CMM as the ultimate goal.

For the People domain, the organisational type and what prevailing regulatory requirements may apply or affect them were considered (shown as the Organisation Type). It was determined (based on previous experience in working with such entities) that each organisation type would have different requirements regarding employment, training, career development, and staff retention policies and requirements. Additionally, the levels of accountability, competency, and proficiency testing of personnel varied based on organisation type.

Furthermore, although employment, promotion, and other personnel practices would vary between organisations, a fundamental set of baseline criteria could be created based on best practices and ISO 17025/ASCLD-LAB requirements to create a sound foundation and set of practices that could be applied to an organisation regardless of its type. This foundation would also serve as the basis for implementing P-CMM within the organisation and enabling the various reporting and assessment features incorporated into the knowledge base set of standard operating procedures.

Organisation type and its regulatory requirements may affect how effectively personnel are trained and tested. Their levels of proficiency would ultimately affect the organisation's digital forensics People-Capability Maturity (P-CMM).

The key People elements were identified (shown as Key Elements) in Figure 10. The key process element of the People domain was identified and used as the basis to create the *DF-C²M² Skills Competency Testing and Skills Matrix* and related assessment tool.

Another key finding during this research was that there were no common, well-defined, or structured job roles, job descriptions, or training and career development plans that addressed the various roles typically found within an established digital forensic lab.

To that end, 6 possible technical roles were identified (during assessments of Lab #1 and Lab #2 that could possibly apply to other digital forensic labs of any organisational type and regardless of whether they were accredited or planned to achieve ISO 17025 accreditation. The six key People elements identified are:

1. **Digital Forensic Trainee** – Typically a new recruit under initial training who has yet to pass any internal basic competency and proficiency tests related to Six Steps Model Phase 2 (Collection) and primarily includes evidence receipt, chain of custody, basic device disassembly, media preparation, and basic imaging functions. Works under close supervision.

2. **Forensic Engineer (technician)** – Typically an individual who has proven competency in basic digital forensic lab technical and non-technical processes related to evidence handling, media imaging, workstation preparation and verification, and device disassembly and re-assembly. May also assist with examination pre-processing tasks working under the supervision of a senior forensic examiner.

3. **Forensic Examiner (in a specific sub-discipline)** – Typically an individual who has undergone at least 12 to 18 months in the role as a forensic engineer (technician), and has undergone additional product-specific and process-specific training as defined within the DF-C²M² Training Manual and Forensic Examiner

Career Development Manual (see Body of Knowledge - Process Domain document). Additionally, this individual will have completed at least 5 test examinations, working under close supervision, and will have passed all internal competencies and external proficiency tests. Examiners may be classed into specific roles based on their training and career development paths such as the computer forensic examiner, mobile forensic examiner, etc.

4. **Senior Forensic Examiner** – Typically has completed at least 5 years as a digital forensic examiner, has been trained on more advanced digital forensic subject (known as Specialists) with the *DF-C$^{2}$M$^{2}$ Training Progression Plans,* and has been recognised as an expert witness by at least one judicial authority.
5. **Digital Forensic Specialist** – Typically, this individual will have completed their specialised training and career development track and have at least 3 years as a senior forensic examiner.
6. **Digital Forensic Management**– This may include roles such as lab manager, quality manager, administrative staff, and non-digital forensic technical staff such as IT support team.

NB: The above roles identified (whilst not exhaustive) in and the absence of industry standard defined roles were felt by participants to be generic enough to be applied to most digital forensic organisations. Other issues cited during this research was that the lack of common, structured career development and progression plans across digital forensic labs (which, it could be argued stems from the lack of industry wide defined job roles) meant that there was no easy way to equate a digital forensic engineer in one lab versus one in another, for example.

Therefore, for each role listed above, a bespoke set of training, skill progressions, and assessment and planning criteria were created with the DF-C$^{2}$M$^{2}$ Planning and Assessment Tool. The People elements identified within the DF-C$^{2}$M$^{2}$ included both technical and non-technical knowledge, skills, and core competencies that would need to be sufficiently documented to enable the organisation to maintain a standard level of skills and process knowledge to enable both compliance with ISO 17025 and assessment via the People Capability Maturity Model (P-CMM).

Next, the constraints (shown as Challenges) that the above sub-elements created were identified and assessed. For the People sub-elements, the key Challenges and constraints identified during this research were categorised as:

i). **Training** – The following areas were assessed regarding training during the research that was largely ignored by other models reviewed in Chapter 2. Key challenges that needed to be addressed included: On-the-Job vs. Instructor-led training, justifying training Costs vs. Benefits, structured uniform training based on job role and career progression, and technical and non-technical training (e.g. training on processes related to Health and Safety operations, etc.).

As a result, a well-defined set of career development guides, skill progression charts, and job descriptions (aligned with industry best practices and ISO 17025 requirements) were created to serve as the basis for assessments and planning, as well as part of the People component of the DF-C$^2$M$^2$ Knowledge Base.

ii). **Certification** – The need to keep the certifications of personnel current was often cited as a challenge both by practitioners and lab management. The issues with certifications were also explored in Chapters 1 and 2, and remedial items were included to address the shortcomings of traditional product-specific training and certifications.

iii). **Competency and Proficiency Testing** – The need for internal competency tests (ISO/IEC: 17025:2005) and their limitations were identified in Chapter 2, and issues related to external proficiency tests or the lack thereof (e.g. mobile forensics) were also identified in Chapter 2. None of these essential ISO 17025/ASCLD-LAB requirements were addressed in the various frameworks and models reviewed in Chapter 2.

**iv). Career Development Planning and progression** – The lack of a unified approach to career development and progression for an emerging science such as digital forensics stands as a distinct barrier towards its acceptance as a ‘true forensic science’ in the view of several traditional forensic science practitioners.

Forensic Readiness was identified during this research as a key managerial concern across all organisational types assessed. Forensic Readiness contributed towards a significant part of the assessment and planning requirements.

Of the existing models reviewed, only one referred briefly to the need to include a comprehensive set of People elements in digital forensic and incident response readiness frameworks on an equal level to that of Tools and Processes.

Finally, the objective for each key element was defined, i.e. People Capability Maturity was defined as the ultimate objective (Objective), and therefore key elements of P-CMM were factored into all process elements. Ultimately, People Capability Maturity would contribute towards the final goal of Digital Forensics Organisational Capability Maturity.

### 5.6.1 DF-C²M² People Domain Outputs

#### 5.6.1.1 Competency Test Process, Forms & Skills Matrices

To address issues related to the lack of a common means of effective competency testing of skills, the DF-C²M² Competency Test Processes and Skill assessment matrices were created. These tests and skills matrices were aligned with the model job descriptions to help assess and determine the required technical skills and competencies required for each role within a typical digital forensic lab.

The competency tests (ISO/IEC: 17025:2005) as defined within ISO 17025 (section 5.2.6.2) were created and designed on common tasks that would typically be performed as part of a digital forensic examination and as required ISO 17025 technical assessments/witnessing of tasks.

The competency tests were designed to witness and document lab personnel capture and preserve digital evidence and media for devices types typically covered within a lab’s scope of accreditation, and these were:

a). Hard drive preservation, imaging, verification and write protection

b). Diskette preservation, imaging, verification and write protection

c). Mobile Phone preservation and data extraction

d). SIM card extraction and cloning

e). MicroSD card media preservation, imaging, verification and write protection

f). CD/DVD imaging and verification

g). USB device preservation, imaging and verification

These tests would use a variety of common digital forensic tools, and the process used to perform the various tasks being witnessed should conform to digital forensics best practices such as the use of write-blockers, recording of MD5 hashes and technical notes. The tests also test the participant's ability to explain the technical processes and theory behind the use of the tools and methods. The skills matrices were designed to cover specific skill sets and knowledge rated against a set of criteria that were aligned to the P-CMM levels (1 to 5).

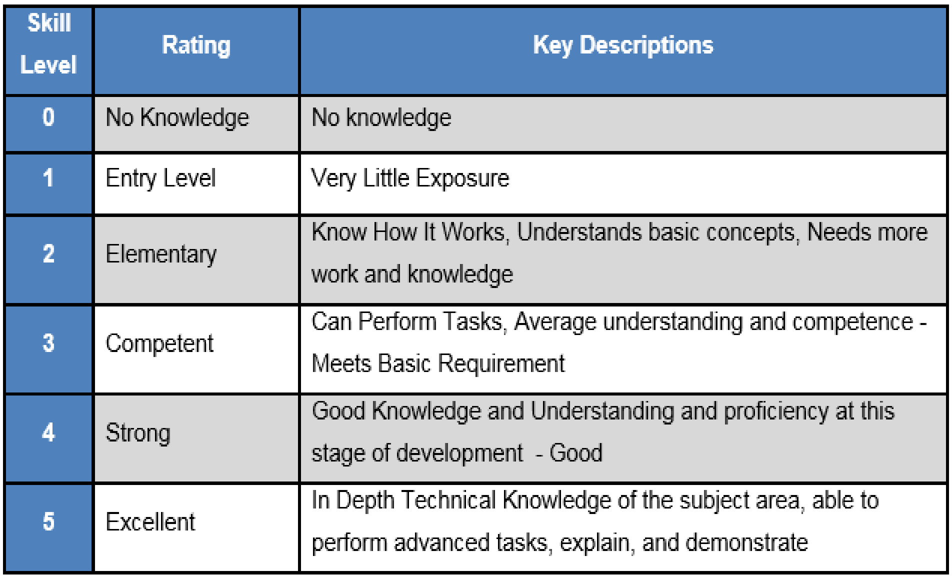
A skills matrix for new digital forensic engineers covering essential elements was created. The key essentials for this role included:

1. IT Fundamentals (Hardware and Software)
2. Forensic Principles/Introduction
3. Computer Forensics Fundamentals
4. Mobile Phone Forensics Fundamentals
5. Use of Primary Forensic Tools (Computer and Mobile)
6. Operating Systems – Core Technical Knowledge
7. Lab Quality, Operational, Health & Safety and Technical Processes

Note that Lab Quality processes as per requirements defined within ISO 17025 require that individuals employed by an accredited lab subscribe to the Lab's Code of Conduct and legal requirements (ISO/IEC: 17025:2005). Typically, the Lab's Code of Conduct will also include ethics and legal requirements. The Body of Knowledge Process Domain Quality Management section contains sample Code of Conducts, Legal and ethical requirements.

Furthermore, the criteria for determining overall People Capability Maturity (P-CMM) were designed and included. The following ratings were used to rate knowledge in each area assessed as shown in Table 11:

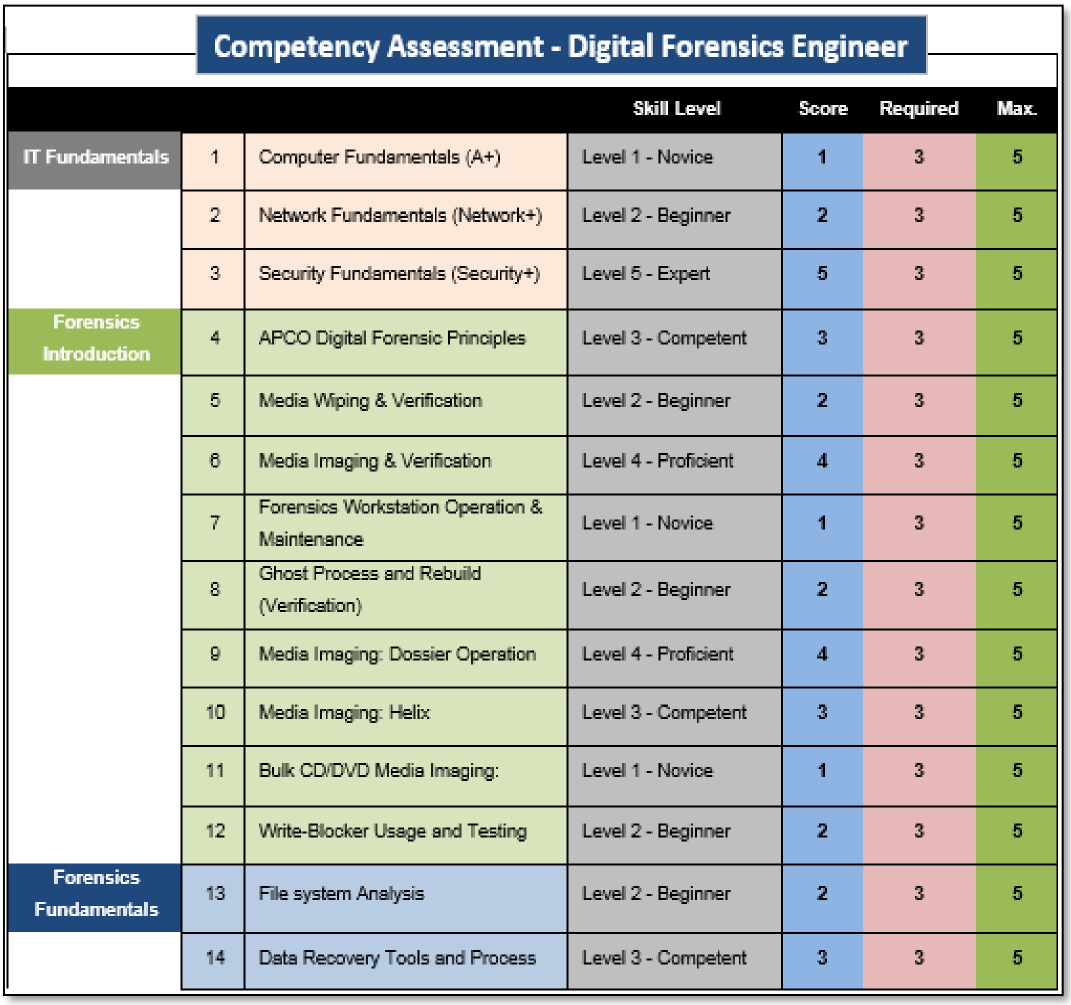
**Table 11: Skill matrix rating – aligned to P-CMM**



| Skill Level | Rating | Key Descriptions |
|---|---|---|
| 0 | No Knowledge | No knowledge |
| 1 | Entry Level | Very Little Exposure |
| 2 | Elementary | Know How It Works, Understands basic concepts, Needs more work and knowledge |
| 3 | Competent | Can Perform Tasks, Average understanding and competence - Meets Basic Requirement |
| 4 | Strong | Good Knowledge and Understanding and proficiency at this stage of development - Good |
| 5 | Excellent | In Depth Technical Knowledge of the subject area, able to perform advanced tasks, explain, and demonstrate |

For each assessed member of staff, the following form would be used to record findings as per the sample below. The assessment would include the candidate's rating versus the minimum required rating for each of the respective areas being assessed. Using this tool, a team average could be determined to assist with benchmarking and determining overall team competency, as illustrated in Table 12.

Table 12: Sample trainee skills matrix extract



Competency Assessment - Digital Forensics Engineer

| | | | Skill Level | Score | Required | Max. |
|---|---|---|---|---|---|---|
| IT Fundamentals | 1 | Computer Fundamentals (A+) | Level 1 - Novice | 1 | 3 | 5 |
| | 2 | Network Fundamentals (Network+) | Level 2 - Beginner | 2 | 3 | 5 |
| | 3 | Security Fundamentals (Security+) | Level 5 - Expert | 5 | 3 | 5 |
| Forensics Introduction | 4 | APCO Digital Forensic Principles | Level 3 - Competent | 3 | 3 | 5 |
| | 5 | Media Wiping & Verification | Level 2 - Beginner | 2 | 3 | 5 |
| | 6 | Media Imaging & Verification | Level 4 - Proficient | 4 | 3 | 5 |
| | 7 | Forensics Workstation Operation & Maintenance | Level 1 - Novice | 1 | 3 | 5 |
| | 8 | Ghost Process and Rebuild (Verification) | Level 2 - Beginner | 2 | 3 | 5 |
| | 9 | Media Imaging: Dossier Operation | Level 4 - Proficient | 4 | 3 | 5 |
| | 10 | Media Imaging: Helix | Level 3 - Competent | 3 | 3 | 5 |
| | 11 | Bulk CD/DVD Media Imaging: | Level 1 - Novice | 1 | 3 | 5 |
| | 12 | Write-Blocker Usage and Testing | Level 2 - Beginner | 2 | 3 | 5 |
| Forensics Fundamentals | 13 | File system Analysis | Level 2 - Beginner | 2 | 3 | 5 |
| | 14 | Data Recovery Tools and Process | Level 3 - Competent | 3 | 3 | 5 |

Additionally, for each candidate, a skills matrix showing required vs. actual knowledge of key knowledge areas was created as shown in Figure 9:

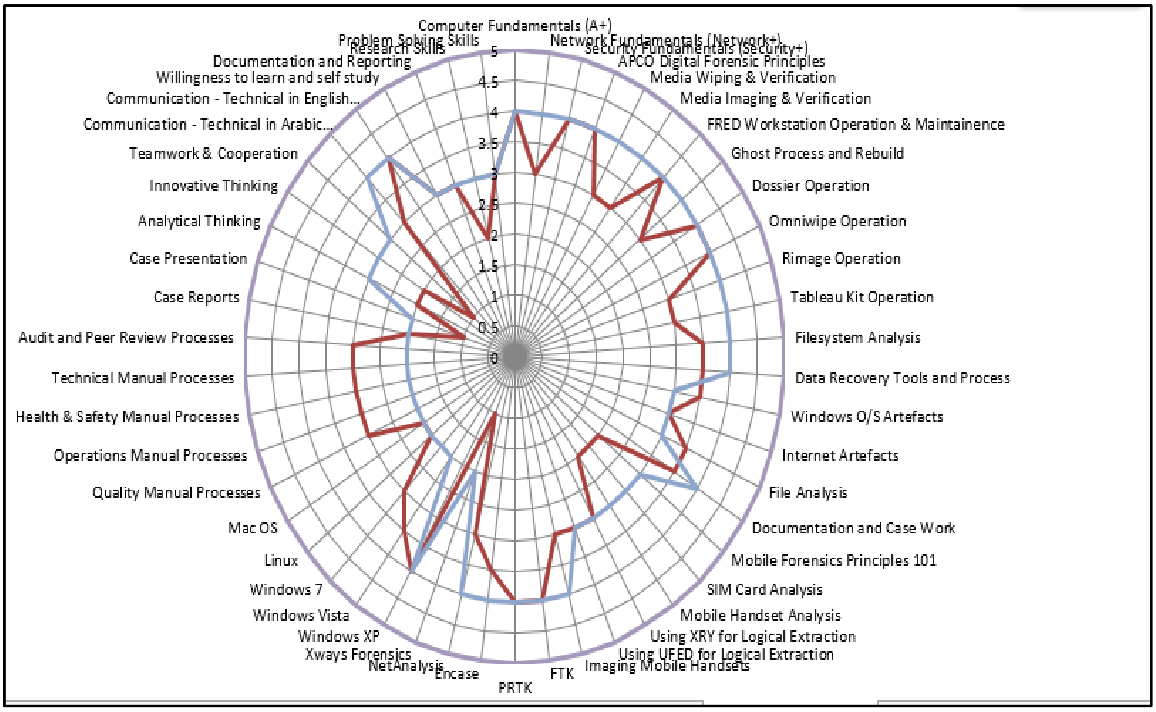
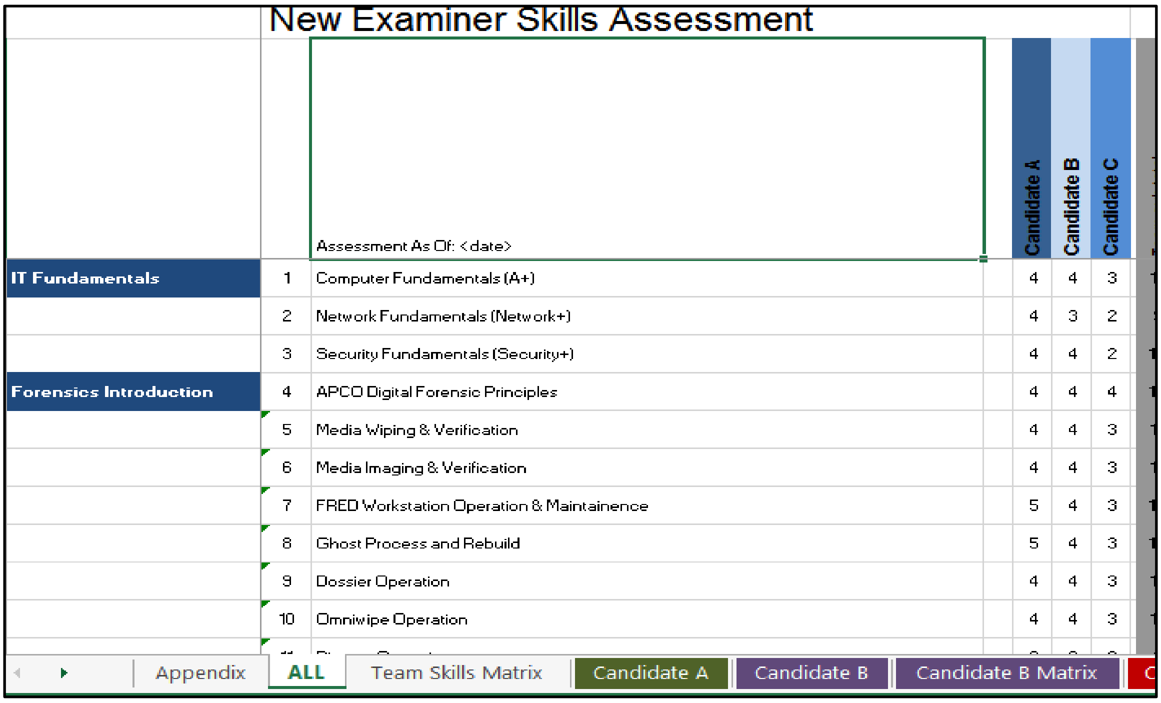


Figure 9: Sample skills matrix mapping: actual vs. required skills level

Provision for comparisons ratings of staff for each job role was provided for to enable staff assessment and team assessments in all key areas as per the sample in Figure 10:



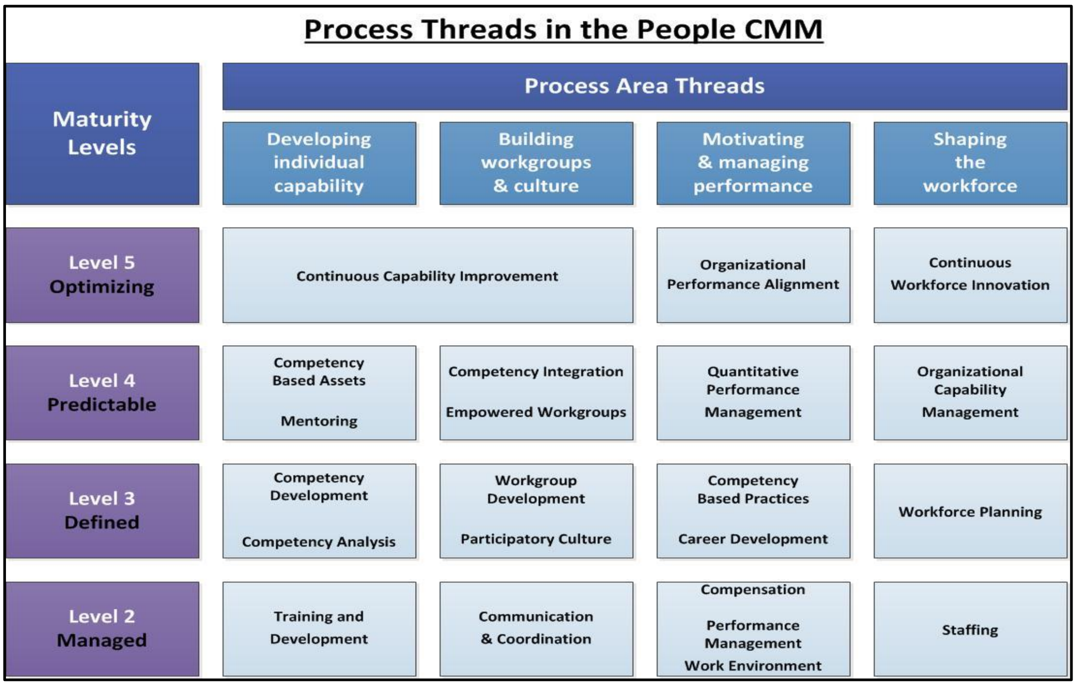
New Examiner Skills Assessment

| | | | Candidate A | Candidate B | Candidate C |
|---|---|---|---|---|---|
| | | Assessment As Of: <date> | | | |
| IT Fundamentals | 1 | Computer Fundamentals (A+) | 4 | 4 | 3 |
| | 2 | Network Fundamentals (Network+) | 4 | 3 | 2 |
| | 3 | Security Fundamentals (Security+) | 4 | 4 | 2 |
| Forensics Introduction | 4 | APCO Digital Forensic Principles | 4 | 4 | 4 |
| | 5 | Media Wiping & Verification | 4 | 4 | 3 |
| | 6 | Media Imaging & Verification | 4 | 4 | 3 |
| | 7 | FRED Workstation Operation & Maintainence | 5 | 4 | 3 |
| | 8 | Ghost Process and Rebuild | 5 | 4 | 3 |
| | 9 | Dossier Operation | 4 | 4 | 3 |
| | 10 | Omniwipe Operation | 4 | 4 | 3 |

Figure 10: Skills comparison per job role

### 5.6.1.2 Incorporating People Capability Maturity (P-CMM) Assessment Tools and Criteria

Through witnessing and assessing competency tests and interviews, P-CMM ratings were derived for the lab that was assessed based on competency tests, skills assessments, and level of detail shown in documenting process materials as per the P-CMM Process Threads in Figure 11.



Process Threads in the People CMM

| Maturity Levels | Process Area Threads | | | |
|---|---|---|---|---|
| | Developing individual capability | Building workgroups & culture | Motivating & managing performance | Shaping the workforce |
| Level 5 Optimizing | Continuous Capability Improvement | | Organizational Performance Alignment | Continuous Workforce Innovation |
| Level 4 Predictable | Competency Based Assets<br>Mentoring | Competency Integration<br>Empowered Workgroups | Quantitative Performance Management | Organizational Capability Management |
| Level 3 Defined | Competency Development<br>Competency Analysis | Workgroup Development<br>Participatory Culture | Competency Based Practices<br>Career Development | Workforce Planning |
| Level 2 Managed | Training and Development | Communication & Coordination | Compensation<br>Performance Management<br>Work Environment | Staffing |

Figure 11: Process threads in the people CMM (source: P-CMM SEI)

The DF-C²M² assessment tool includes assessment checklists and criteria to map both Capability Maturity and People Capability Maturity levels as part of the assessment and DF-C²M² knowledge base.

The P-CMM ratings covered additional criteria based on the P-CMM with specific assessment criteria for multiple domains within P-CMM including:

- Staffing
- Communication & Coordination
- Work Environment
- Performance Management
- Training
- Compensation
- Competency Analysis

- Workforce Planning
- Competency Development
- Career Development
- Competency-Based Practices
- Workgroup Development
- Participatory Culture

#### 5.6.1.3 DF-C²M² Training and Career Progression Plan for Digital Forensics

The lack of structured training plans, and prerequisite skills requirements per job role, has led to the lack of common, structured career development and progression plans within many labs.

Job analysis of the various roles and tasks that structured career training and development plans were created to enable progression from one level to the next in a structured, planned manner. Rather than simply stating sets of skills that were required, the skills requirements were mapped to currently available training courses that would address the skills and knowledge requirements, and where possible, the course synopsis were used to indicate courses that should be taken (or equivalent) to fulfil the training and career progression requirements of the participant lab.  Each course synopsis/outline together with learning objectives and outcomes would be checked to as an indicator that the required skills or knowledge is covered within a given course.

For each candidate and job role, a prescriptive custom Career Development Plan could therefore be easily created detailing on-the-job training, mentoring, and self-study assignments with target completion dates, and assessment requirements to support the completion of each stage of the career progression plan. The DF-C²M² Career Development Plan is included within the DF-C²M² Body of Knowledge and would also be subject to annual reviews and updates as may be required together with related job descriptions.

The DF-C²M² People domain addresses the issues cited during the initial stages of the research as well as issues identified during the assessment and evaluation of existing labs. The People domain provides a means whereby an organisation can implement, measure, and improve upon the People Capability Maturity in unison with their Process Capability Maturity via the DF-C²M² model.

## 5.7 DF-C²M² - TOOLS DOMAIN

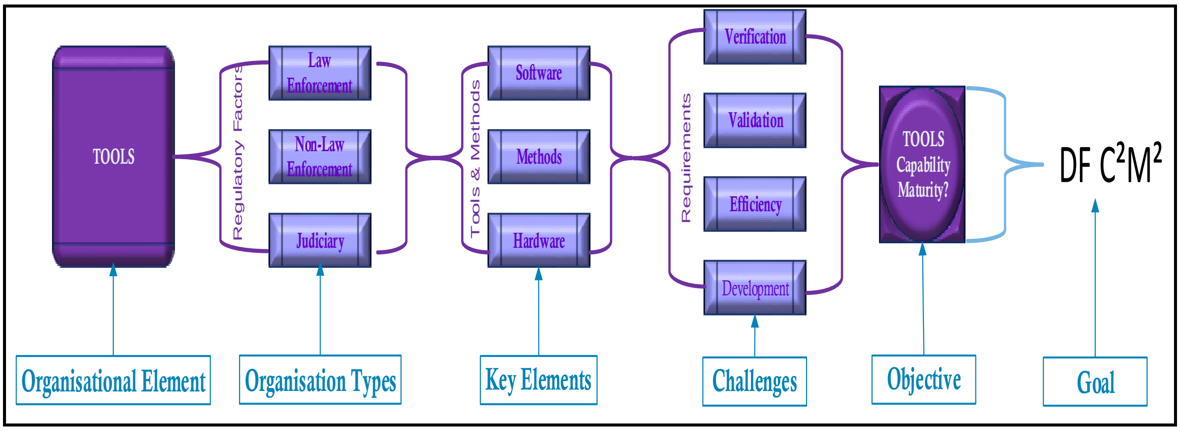


Figure 12: TQM analysis of DF-C²M² tools domain challenges

For the Tools domain, the organisational type and what prevailing regulatory requirements may apply to affect them were considered (shown as the Organisation Type). It was therefore decided that each organisation type may have different requirements regarding the tools used, tool validation and verification requirements, and audit requirements depending on the types of cases they may be required to process (Civil, Criminal, Internal Policy violations, etc.) as per the TQM Analysis in Figure 12.

Additionally, any levels of compliance with prevailing internal or external regulatory requirements would vary from one organisation type to another. Such requirements would ultimately affect how the organisation works and whether or not it is are compelled to follow existing quality management and digital forensics standards in addition to trying to achieve organisational maturity.

The key Tools elements were identified (shown as Key Elements). The key process elements of the Tools Domain that were identified are:

- **Software** - programs, firmware, and utilities used to prepare, extract, decode, and report on digital forensic evidence.
- **Methods** – methods used to test and validate tools and non-technical processes within the scope of the DF-C²M².
- **Hardware** – physical and technological devices used to prepare, extract, process, or preserve the integrity of digital evidence.

For each sub-element listed above, a bespoke set of assessment and planning criteria were created with the DF-C$^2$M$^2$ Planning and Assessment Tool.

The Tools elements identified included both tools and methods that would need to be sufficiently documented, validated, and verified to enable the organisation to maintain a standard unified method of processing examinations, and to enable admissibility of derivative evidence, compliance with ISO 17025, and efficiency of tools and methods as defined within DF-C$^2$M$^2$ Tools Capability Maturity.

- Additionally, a key Tools service planning and assessment tool was created within the DF-C$^2$M$^2$ Service Catalogue to help to identify all services that a digital forensics laboratory may be required to provide and to help to determine their inter-relationships and dependencies.

- The initial costs of implementing a service based on acquiring new tools was included in the DF-C$^2$M$^2$ Service Catalogue Impact vs. Complexity calculations, and the ongoing maintenance cost of such tools was also factored into the DF-C$^2$M$^2$ Service Catalogue.

Next, the constraints shown as Challenges in Figure 12 indicate that the above sub-elements created were identified and assessed. These challenges were identified and often cited as issues during the interviews and surveys with practitioners. For the Tools sub-elements, the key Challenges and constraints identified were categorised as:

i). **Verification:** The need for tool (hardware and software) testing and verification prior to commencement of each examination as per ISO 17025/ASCLD-LAB requirements. Verification of hardware and software tools would be required prior to the start of each case as per ISO 17025 requirements (ISO/IEC: 17025:2005).

ii**). Validation:** The need for tools to have been validated using criteria and test data sets similar to those used by NIST Computer Forensic Tool Testing (CFTT). Tool and method validation would be required when a new tool or a new version of an existing tool is to be tested and approved for use within the lab as per ISO 17025 requirements (ISO/IEC: 17025:2005).

The challenges in validating tools against sufficiently robust criteria have proved to be a challenge for many labs. Additionally, the time and cost overhead that tool validation often entails - may sometimes mean that labs would rather make do with older versions of tools and their deficiencies rather than investing in validating newer versions themselves.

iii). **Efficiency** – Accuracy and performance of tools was highlighted as a major issue amongst the digital forensic practitioners assessed. The need to find and share information on the most efficient tools for a given set of analysis tasks, and how best to utilise and optimise the efficiency of digital forensic tools was factored into the design aspects of the DF-C$^2$M$^2$ and as part of the proposed DF-C$^2$M$^2$ community sharing facility and knowledge base.

iv). **Tool and Method Development** – Resource constraints and skills (such as programming skills) were cited as limitations by several practitioners. Tool development was often also cited as too time-consuming and therefore costly by managers.

Many practitioners stated that they looked forward to a forum where collaborative research could be done using shared tools and resources to help speed up the process and for a repository of previously conducted research for reference purposes (see Appendix D – *Extracts of Interviews*).

Finally, the objective for each key element was defined, i.e. Tools Capability Maturity was defined as the ultimate objective (Objective), and therefore key elements of CMM were factored into all Process elements.

### 5.7.1 DF-C$^2$M$^2$ Tools Domain Outputs

Key elements of the Tools domain included detailed process and technical workflows, and standard operating procedures related to tool verification, tools, and methods validation. Additionally, the DF-C$^2$M$^2$ Service Catalogue enables managers to determine the tools and prerequisites for delivery of each service. The skills training and progression plans were designed to incorporate training and competency tests for the most commonly used forensic tools for each forensic specialisation area such as computer forensics. These training plans also included non-product-specific training requirements such as File Systems Analysis and Digital Evidence handling.

Based on feedback during the research, the DF-C$^2$M$^2$ will propose tools testing forum that will enable laboratories to share the burden of tool validation through collective testing and sharing of data amongst DF-C$^2$M$^2$ participant labs. A key output of the tools domain is the DF-C$^2$M$^2$ Body of Knowledge, which was created, in part, to help address the lack of a central repository of digital forensics policies, processes, and best practices as they relate to the People, Processes, and Tools domains.

### 5.7.2 Df-C$^2$M$^2$ – The Body of Knowledge

The DF-C$^2$M$^2$ Body of Knowledge is a structured collection of digital forensic-specific processes, standard operating procedures, workflows, forms, and guides. The Body of Knowledge provides the basis for building and implementing the People, Processes, and Tools domains within the DF-C$^2$M$^2$, and yet at the same time the Body of Knowledge serves as the main DF-C$^2$M$^2$ planning, implementing, audit, and assessment toolkit.

The Body of Knowledge was designed as the basis for the assessments conducted as part of the research, and to provide participating digital forensics laboratories with a structured and detailed assessment system and best practices repository covering all three key elements (People, Processes, and Tools) of a digital forensic laboratory. The DF-C$^2$M$^2$ Body of Knowledge provides participating organisations with a current and up-to-date compendium related to digital forensics.

In essence, the DF-C$^2$M$^2$ Body of Knowledge was designed to provide the steps, planning guides, and template processes and procedures that can be easily adapted and implemented by new, existing, or ISO 17025 accredited digital forensic labs to achieve digital forensics organisational capability maturity and compliance with existing standards and best practices.

#### 5.7.2.1 Body of Knowledge Design Goals

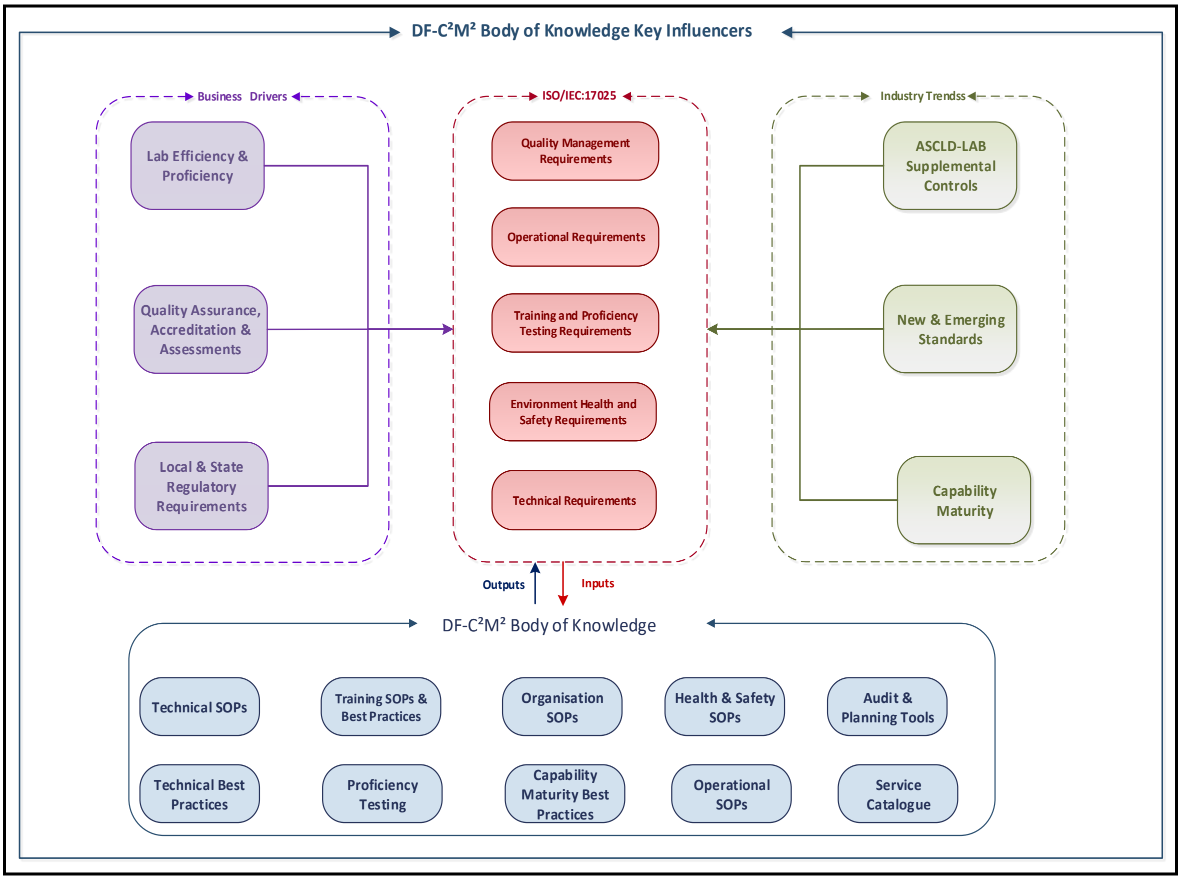
The DF-C$^2$M$^2$ and the related DF-C$^2$M$^2$ Body of Knowledge's design goals were to provide:

1. A detailed list of requirements to cater to the majority of requirements for most digital forensic labs (including those in law enforcement).
2. A common model that can be used to assess all digital forensic labs of a similar nature, e.g. law enforcement vs. law enforcement, commercial vs.

commercial, etc. and a modular framework that would enable organisations to either:

A. Achieve international accreditation of their digital forensics laboratory and operations (Applicable to new and existing labs).
B. Improve on current systems and processes (Applies to new and existing labs).
C. Create a shared framework and repository of knowledge for participating organisations.

The schematic in Figure 13 depicts the DF-C²M² Body of Knowledge Key Influencers, illustrating that the Body of Knowledge is designed to cater to changes in requirements and be readily updated accordingly.



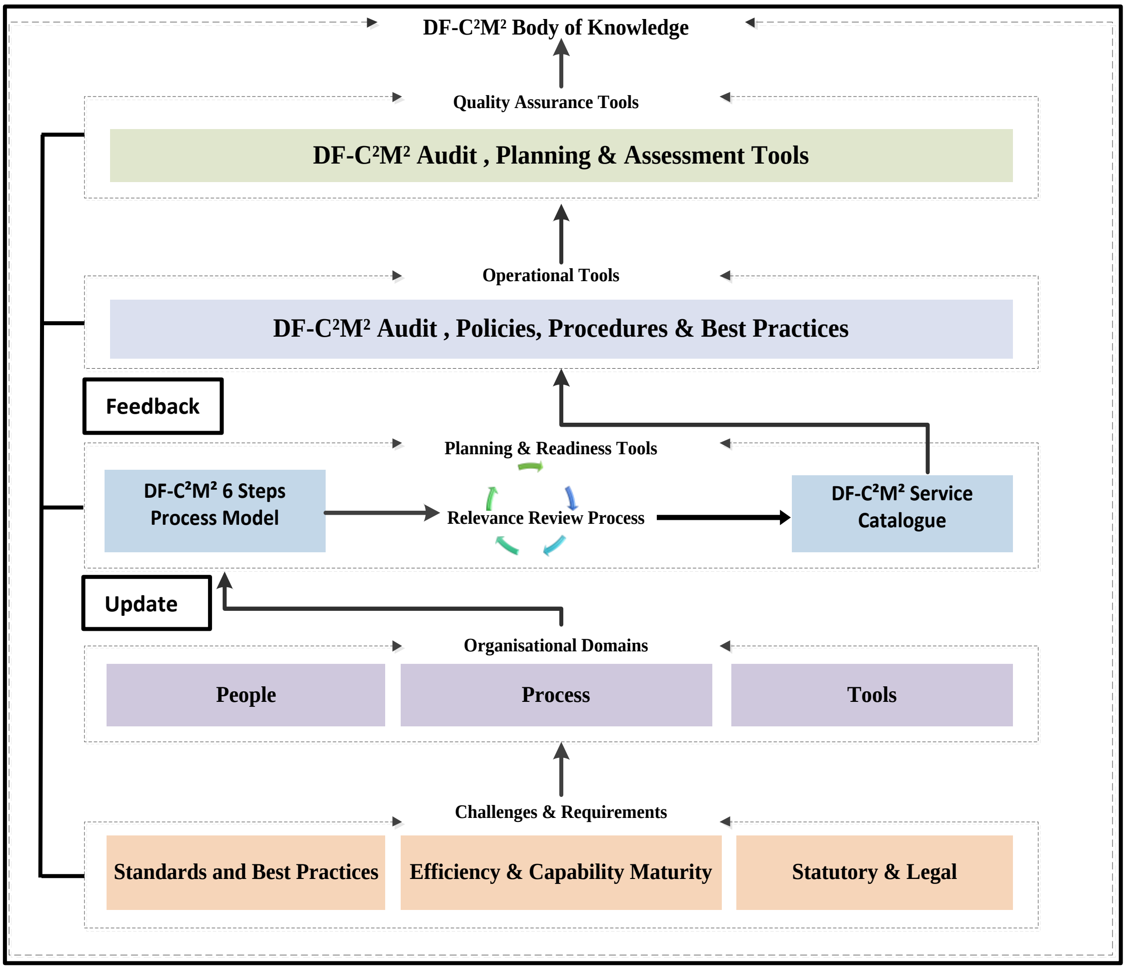
DF-C²M² Body of Knowledge Key Influencers
Business Drivers
Lab Efficiency & Proficiency
Quality Assurance, Accreditation & Assessments
Local & State Regulatory Requirements
ISO/IEC:17025
Quality Management Requirements
Operational Requirements
Training and Proficiency Testing Requirements
Environment Health and Safety Requirements
Technical Requirements
Industry Trends
ASCLD-LAB Supplemental Controls
New & Emerging Standards
Capability Maturity
Outputs
Inputs
DF-C²M² Body of Knowledge
Technical SOPs
Training SOPs & Best Practices
Organisation SOPs
Health & Safety SOPs
Audit & Planning Tools
Technical Best Practices
Proficiency Testing
Capability Maturity Best Practices
Operational SOPs
Service Catalogue

Figure 13: DF-C²M² body of knowledge key influencers

Figure 13 illustrates the key influencers that helped to determine which elements are added and/or modified within the Body of Knowledge. Ultimately, for the Body of Knowledge to be practical and relevant in the long term, it would have to take into account three key environmental factors, namely Business Drivers, Standards, and

Industry Trends based on practitioner inputs. These three categories of influencers would affect the usefulness and relevance of Body of Knowledge components in its present state and in the future.

Figure 14 illustrates how industry Challenges and Requirements (derived from Influencers in Figure 13) were evaluated for relevance and impact on the People, Processes, and Tools domains.



DF-C²M² Body of Knowledge
Quality Assurance Tools
DF-C²M² Audit , Planning & Assessment Tools
Operational Tools
DF-C²M² Audit , Policies, Procedures & Best Practices
Feedback
Planning & Readiness Tools
DF-C²M² 6 Steps Process Model
Relevance Review Process
DF-C²M² Service Catalogue
Update
Organisational Domains
People
Process
Tools
Challenges & Requirements
Standards and Best Practices
Efficiency & Capability Maturity
Statutory & Legal

**Figure 14: DF-C$^2$M$^2$ components design inter-relationship**

Next, these requirements were translated into tangible items that could be used to help determine new requirements or changes to the Six Steps Model, and whether these changes may require revisions to the Service Catalogue (list of services or prerequisites). These requirements were evaluated to determine which categories of Tools (Operational, Quality Assurance, etc.) would be affected and need to be revised in order to accommodate this change.

The Body of Knowledge consists primarily of content created to address perceived needs of a digital forensic lab seeking to gain ISO 17025 accreditation, and work towards achieving Capability Maturity. The content was used initially as the basis for the creation of the assessment tool, and the design of the DF-C$^2$M$^2$ key elements. The content was updated at various stages during the research based on new findings, improved workflow designs, and feedback from participant labs.

A summary of the key elements and their creation is outlined below in Table 13:

**Table 13: BoK key elements and their creation**

| BoK Component | Function | Created | Comment |
|---|---|---|---|
| Technical Workflows | To depict detailed technical processes | ✓ | |
| Process Workflows | To illustrate non-technical processes and procedure based on ISO 17025 requirements | ✓ | Includes input from assessed lab participants |
| Assessment Tool | Covers all aspects of ISO 17025 with ASCLD-LAB Supplemental requirements, CMM, P-CMM, Skills , Training and overall audit requirements | ✓ | Included in evaluation and review with assessed labs |
| Technical and procedural forms | To structure and capture vital records and information for each process | ✓ | Included in evaluation and review with assessed labs |
| Training Progression plans and Workflows | Structured, suggested training required per role based on skill/job analysis and training requirements mapping performed | ✓ | Includes input from assessed lab participants |
| Competency tests for technical processes | Specific, task oriented competency tests, to test the technical and procedural knowledge of a candidate in accordance with ISO 17025 requirements | ✓ | Included in evaluation and review with assessed labs as part of witnessing of tests for skills/job analysis requirements |

| BoK Component | Function | Created | Comment |
|---|---|---|---|
| Tools Domain & Technical procedures | Technical workflows covering all technical processes and tool validation requirements. Supplements Process Domain BoK elements related to verification and validation of tools and methods with CMM and ISO 17025 elements included. Standard technical processes also included in Process Domain BoK | ✓ | Includes input from assessed lab participants |
| Process Domain | Collection of Processes related to Quality Management, Lab Operations, Health & Safety, and Technical procedures with C-MM and ISO 17025 elements included. | Previously created as part of Lab #1 initial process documentation set, updated | Researcher was previously director responsible for establishment, and creation of LAB#1, including systems, processes and controls. |
| People Domain | Trainings, skills requirements and career development plans, with P-CMM and ISO 17025 elements included | ✓ | |
| External best practices | External NIST, NIJ, SWGDE and APCO Best practices referenced throughout where applicable. | No | Referenced |

Additionally, although the Body of Knowledge core is to provide tools for each of the three key domains of People, Processes, and Tools, Figure 14 illustrates that the Body of Knowledge tools can be further categorised based on three core functions: Planning Tools, Operational Tools, and Quality Assurance Tools – which is how most practitioners would tend to view digital forensic lab design and operations. The Body of Knowledge Reference Tables for People, process and tools domains can be found in Table 14 in Chapter 6.

#### 5.7.2.2 ISO 17025 and 27034 Audits and Assessment Checklists

ISO 17025 readiness and readiness assessment tools were cited as an issue during the research, and to that end, an ISO 17025 audit assessment checklist with ASCLD-LAB supplemental controls was created to assist with the design elements of the DF-C$^2$M$^2$ Quality Management components that extend to all three key domains (People, Processes, and Tools).

Additionally, an overall assessment and rating summary was also designed as a management decision support system to help plan and gauge compliance on a regular basis as part of the DF-C$^2$M$^2$ assessment tool.

Following a review of the ISO 17025 standards and ASCLD-LAB supplemental requirements, an audit assessment planning sheet was created to assist with the review of lab processes and to help determine areas for improvement and capability maturity levels for each area.

The assessment tool covered the ISO 17025:2005 and ASCLD-Lab supplemental requirements to help laboratories demonstrate proof of compliance to determine degree of maturity. The ISO 17025 and 27034 assessment tools are included in the DF-C$^2$M$^2$ Knowledge Base as both a planning and assessment tool.

### 5.7.2.3 Body of Knowledge Six Steps Model-specific Outputs

Processes and tools for use within the Six Steps Model provided within the Body of Knowledge include:

**DF-C²M² Six Steps Model Process Domain Knowledge Base Outputs:**

1. **Assessment:** The Assessment key element consisted of 18 specific planning and audit questions to help assess the capability maturity and ISO 17025 compliance at each level and an overall maturity level rating for this section.
2. **Collection:** The Collection key element consisted of 26 specific planning and audit questions to help assess the capability maturity and ISO 17025 compliance at each level and an overall maturity level rating for this section.
3. **Examination:** The Examination key element consisted of 30 specific planning and audit questions to help assess the capability maturity and ISO 17025 compliance at each level and an overall maturity level rating for this section.
4. **Analysis:** The Analysis key element consisted of 10 specific planning and audit questions to help assess the capability maturity and ISO 17025 compliance at each level and an overall maturity level rating for this section.
5. **Reporting:** The Reporting key element consisted of 12 specific planning and audit questions to help assess the capability maturity and ISO 17025 compliance at each level and an overall maturity level rating for this section.
6. **Review:** The Review key element consisted of 6 specific planning and audit questions to help assess the capability maturity and ISO 17025 compliance at each level and an overall maturity level rating for this section.

## 5.8 SUMMARY

Collectively, the key elements of People, Processes, and Tools and the key sub-elements were identified as issues, and these were identified in reviews of existing standards and forensic models to establish the design foundation of the Digital Forensics – Comprehensive Capability Maturity Model (DF-C$^2$M$^2$).

The DF-C$^2$M$^2$ People, Processes, and Tools elements as defined by the TQM analysis workflow are the critical success factors in enabling an organisation to achieve Digital Forensics Organisational Capability Maturity by combining Process Capability Maturity, People Capability Maturity, and Tools Capability Maturity within a unified standards-focussed modular framework – the DF-C$^2$M$^2$.

The main contribution of this research is to create a comprehensive digital forensics capability and maturity model that address the gaps and opportunities discussed in Chapter 2, that covers the three organisational domains (People, Processes, and Tools) by integrating and adapting the existing CMM models and incorporating them to digital forensic laboratory standards/best practices to help overcome the barriers and gaps as previously identified in Chapter 2.

The DF-C$^2$M$^2$ assessment tool has dual purposes in that it lists the DF-C$^2$M$^2$ requirements for each of the three core domains, and provides a way to measure compliance with these requirements. CMM and P-CMM were included in the assessment and planning tools, and CMM ratings were included in the overall assessment for each of the three key domains (Processes, People, and Tools).

The DF-C$^2$M$^2$ Body of Knowledge (originally designed for the assessments) is a key component of the final deliverable and extracts of the Body of Knowledge have been highlighted in this summary. The DF-C$^2$M$^2$ assessment tool forms an integral part of the DF-C$^2$M$^2$ framework and Knowledge Base. The Assessment tool is included as part of this research for review and feedback.

This chapter highlights the key elements of the DF-C$^2$M$^2$ and considerations used in evaluating currently available standards and in evaluating present strengths, weaknesses, and opportunities to serve as the foundation for a more encompassing digital forensics-specific model, the DF-C$^2$M$^2$.

# CHAPTER 6: DF-C$^2$M$^2$: DEVELOPMENT, ASSESSMENT TOOL & BODY OF KNOWLEDGE

## 6.0 INTRODUCTION

This chapter describes the processes used for the realisation and implementation of the Digital Forensics – Comprehensive Capability Maturity Model (DF-C$^2$M$^2$). It will examine each core section/module within the DF-C$^2$M$^2$ and describe the key elements, building on the key aspects of the DF-C$^2$M$^2$ as introduced in Chapter 5.

This chapter highlights the key assessment tools and methods produced from the research. It demonstrates the inclusion of challenges drawn from Chapters 2 and 5 and presents them as part of the DF-C$^2$M$^2$ foundation and Body of Knowledge tool base.

This chapter will also demonstrate how the modular design of the DF-C$^2$M$^2$ enabled it to be updated to include the requirements for cyber/electronic crime investigation units (as a proof of concept), using the same core principles and methods defined in the DF-C$^2$M$^2$.

Additionally, this modularity could easily enable newer related digital forensic standards, such as ISO 27037 (International Standards Organisation (ISO), 2012), to easily be incorporated into the model.  APCO define Cybercrime as "the use of networked computers or internet technology to commit or facilitate the commission of crime" (Amoo & Thomson, 2009), whilst the UK Home Office include the following within their definition " (…) new offences committed using new technologies, such as offences against computer systems and data, dealt with in the Computer Misuse Act of 1990" (Home Office, 2010).

The inclusion of skills and training requirements for cybercrime investigators was to a demonstrate of the expandability of the model, and how inter-related disciplines such as Digital Forensics and Cyber/Electronic crime Investigation can both benefit from shared standards and best practices within the DF-C$^2$M$^2$ framework.

A major challenge cited by many during the research as covered in Chapter 1 was how to assess a lab’s current compliance and capability maturity posture vs. its goals. One method to do that was to design a tool that could be used to help determine and benchmark this information. Additionally, of the various models and frameworks reviewed in Chapter 2, none of the models provided a tool or tangible means to help assess, plan, or benchmark the lab’s current digital forensic status and compliance within that model or framework.

Additionally, practitioners often cited the lack of a central point of reference or common Body of Knowledge that could be used as a guide to assist with the quality assurance and technical issues they typically faced.

To that end, the DF-C$^2$M$^2$ was created, initially as a set of tools to assist with the research, but later as a body of knowledge that those new and established digital forensic labs could use as a navigational aide and as a quality management decision support system.

The DF-C$^2$M$^2$ consists of three key elements; these are:

1. The DF-C$^2$M$^2$ Framework (described in Chapter 1)
2. The DF-C$^2$M$^2$ Body of Knowledge
3. The DF-C$^2$M$^2$ Assessment and Planning Tool.

## 6.1 THE DF-C$^2$M$^2$ BODY OF KNOWLEDGE

The DF-C$^2$M$^2$ Body of Knowledge provides a structured, aggregated repository of written tools, processes, workflows, and best practices that service the requirements of the People, Processes, and Tools domains.

In keeping with the conventional view of a body of knowledge, the DF-C$^2$M$^2$ Body of Knowledge essentially provides a foundation that perhaps in the future could be used as the basis for helping to further establish digital forensics as a true scientific profession.

While the DF-C$^2$M$^2$ Body of Knowledge may be viewed as a key DF-C$^2$M$^2$ tool, it is important to stress that it provides detailed information, and tools to assist with establishing and continuing improvement of the People, Processes, and Tool domains within a digital forensic laboratory.

The Body of Knowledge was initially developed as a means to assist with planned lab assessments during the research, and it later evolved into a key component of the DF-C$^2$M$^2$ conceptual framework and philosophy. For example, it was felt that the results of the DF-C$^2$M Assessment Tool (ISO 17025 and CMM) without reference to a common body of knowledge would be less useful to participating labs and practitioners.

Many elements of the Body of Knowledge were created as part of the research in order to address issues discovered during the interviews and lab assessments. Other elements of the Body of Knowledge were created as a means to incorporate Capability Maturity requirements and guidelines into standard digital forensic lab processes; for example, in the annual assessing and rating of digital forensic examiners, criteria related to compliance with service levels, capability maturity, demonstrated technical expertise, and the number of corrections/omissions in selected previous case work were factored into the DF-C$^2$M$^2$ Personnel Rating matrix, thus providing a method to retrospectively assess an examiner's Capability Maturity.

Additionally, the existing lack of a common body of knowledge related to the various digital forensics areas covered by the assessment tool would not enable participating labs to easily improve their current Capability Maturity and ISO 17025 compliance without the need for extensive and somewhat costly external consulting –

both of which were cited as barriers to achieving accreditation and improved Capability Maturity during assessments and interviews. In many instances, remedial, prescriptive references provided by the DF-C²M² Assessment tool refer to the DF-C²M² Body of Knowledge/body of knowledge as a guide to practitioners, and as such, it is important to highlight key components of the body of knowledge that were created.

Interdependencies between components exist, and the Quality Management System process is the critical element that inter-connects the various other elements together, acting as the foundation upon which all other elements are derived.

As no known Digital Forensics-Specific bodies of knowledge covering People, Processes and Tools are known to publicly exist, other than feedback from participants that reviewed the Body of Knowledge there is no way to accurately determine its completeness.

### 6.1.1 The Body of Knowledge Key Categories are:

**People:** This includes all policies, procedures, plans, records, skills, and competency and proficiency testing information for all lab personnel. It includes key requirements to implement and measure People Capability Maturity within the scope of digital forensics.

**Process:** This includes all policies, procedures, plans, and standard operating procedure manuals for the Quality Management, Lab Operations, Training Management, Health and Safety, and Technical Examination processes – adapted to include process Capability Maturity requirements. It includes related workflows, forms, checklists, and technical reference guides, where applicable.

**Tools:** This includes all policies, procedures, records, and best practices related to the selection, verification, and testing of tools. It includes related forms, workflows, and procedures, where applicable. It includes criteria to measure the efficiency and capability maturity of tools, as well as use of the tools.

The key components of the Body of Knowledge are categorised based on the three DF-C²M² organisational domains, People, Processes, and Tools, as illustrated in Table 14.

**Table 14: DF-C$^2$M$^2$ body of knowledge - people, processes, and tools categories**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| People | Detailed Job Descriptions and proposed Lab Organisational Structure<br>Section 1.0 | Career Development & Training Plan – Coaching Manual<br>Section 2.0<br>See Process Section 5 | External Certification / Exams<br>Section 2.3 | In House Training<br>Section 2.4 | Assigned Reading Assignments<br>Section 2.5 | Technical Skill Assessment guidelines and Skills Matrices<br>Section 2.6 | Operational and Quality Management ‘Soft Skills’<br>Section 2.7 |
| | Quality Manual<br>Section 2.8 | Health and Safety Manual<br>Section 2.9 | Examination Plan Development<br>Section 2.10 | Development of a Curriculum Vitae<br>Section 2.11 | Legal Issues and Expert Testimony<br>Section 2.12 | Competency Testing Resources for all DF Technical roles<br>Section 2.13 | Code of Conduct and Code of Ethics<br>Section 3 |
| | Provision for Local Regulatory Requirements<br>**Country Specific – add to DF-C$^2$M$^2$ ** | Cyber-crime Investigator Training & Career Progression Section<br>Section 4 | Personnel Recruitment Criteria and Guidelines<br>Sections 5.0 & 1.1 | Training Policies and Procedures Manual)<br>See Process Domain BoK Section 3,4 & 5 | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Process | Quality Management System Requirements Processes<br>Process Domain Section 1 | Lab Operations Requirements and Processes<br>Process Domain Section 2 | Operations Manual<br>Process Domain Section 3 | Health & Safety Requirements and Processes<br>Process Domain Section 4 | Training Management Processes<br>Process Domain Section 5 | Technical Procedures and Processes (Computer, Mobile, Digital Video and Triage)<br>Process Domain Section 6 | DF-C$^2$M$^2$ Service Catalogue<br>Process Domain Section 7 |
| | Capability Maturity (People, Process and Tools) processes built-in to all Process requirements<br>Assessment Tool | Lab Capability Maturity & Performance Management<br>DF-C$^2$M$^2$ Assessment Tool | Research & development processes<br>(Under development) | ASCLD-LAB supplemental requirements – Built into All processes.<br>*** Apply to ASCLD/LAB for official version. | | | |

<table>
<tr>
<td rowspan="2">Tools</td>
<td>Tool and Method Validation Processes and Guidelines<br>Process Domain BoK – Technical Manual Section 13 &amp; Tools Domain BoK – Section 8</td>
<td>Tool Testing and Verification Processes and Guidelines<br>Process Domain BoK – Technical Manual Section 13 &amp; Tools Domain BoK – Section</td>
<td>Technical Best Practices (methods and use of tools)<br>Tools Domain BoK - Section 2 to 7, Section 9 &amp; 10</td>
<td>Case Tracking &amp; Performance Management Tool (CMM) (Excel spreadsheet)<br>Process Domain BoK – Case Tracking Excel spreadsheet – Appendix B</td>
<td>Tool and equipment best practices specifications for Computer Forensics, Mobile Forensics, Digital Video Forensics, Triage and Network Forensics –<br>Tools Domain BoK - Section 2 to 7 Technical Process Work</td>
<td>Tools Capability Maturity and efficiency assessment guidelines<br>Process Domain BoK – Assessment Tool</td>
</tr>
<tr>
<td colspan="2">DF-C²M² Community Validated Tools Criteria and Database (planned/future)<br>***Planned/future Development ***</td>
<td colspan="2">DF-C²M² Community developed and tested tools (planned/future)<br>***Planned/future Development ***</td>
<td>DF-C²M² Assessment Tool<br>Process Domain BoK – Assessment Tool</td>
<td>DF-C²M² Framework<br>*** As part of completed Research ***</td>
</tr>
</table>

Each highlighted Body of Knowledge component in Table 14 includes the relevant workflows, forms, and process documentation as may be required. The result is that the DF-C$^2$M$^2$ Body of Knowledge represents a considerable body of work and know-how accumulated and developed over the course of this research that relates to every aspect of digital forensic lab operations and quality management.

The Key elements of the Body of Knowledge reviewed by participant lab senior representatives as part of the DF-C$^2$M$^2$ implementation included:

- **DF-C$^2$M$^2$ ISO17025 Digital Forensics Sample Policies and Standard Operating Procedures (SOP):**

  Peer-reviewed and contributed to by digital forensics subject matter experts. These would enable organisations to assess their current SOPs against the ISO 17025 standard, and integrate any enhancements that they may benefit from or that may assist with accreditation within the current set of SOPs (such as ASCLD-LAB supplemental requirements).

A summary description of the key elements of the Body of Knowledge reviewed by participant labs are highlighted below, categorised based on the domain they belong to:

**1. People Domain: DF-C$^2$M$^2$ Digital Forensics competency training and assessment guidelines and requirements for various roles.**

As illustrated within the People Domain components in Table 14; this provides comprehensive career development, job descriptions, mentoring, training, certification, and career progression plans (aligned with requirements of ISO 17025/ASCLD-LAB) for the most common roles within a digital forensic lab, from Trainee, Digital Forensic Engineer (technician), through Senior Digital Forensic Examiner (Specialist), and covering related by often overlooked key roles such as Lab Manager, Health and Safety Officer, Quality Manager, etc.

### 2. People Domain: DF-C$^2$M$^2$ Cybercrime Investigator competency training and assessment requirements for various roles

This provides comprehensive career development plans, job descriptions, mentoring, training, certification, and career progression plans for the most common roles within a digital forensic lab, from Cybercrime Researcher through specialised roles such as Cybercrime Open Source Intelligence Analyst.

### 3. People Domain: DF-C$^2$M$^2$ Digital Evidence competency testing and training requirements for Judiciary members

This provides comprehensive training, and certification progression plans (aligned with the current and envisaged requirements from International Prosecution and Judiciary initiatives such as those undertaken by the Global Prosecutors E-learning Network (GPEN) [4], Europol/Interpol, etc.) to enhance the judiciary's knowledge of:

- Understanding and interpreting digital evidence
- Understanding limitations of digital evidence
- Requirements for lab accreditations and benefits of accreditation
- The need for and value of digital forensic personnel proficiency testing, training, and certifications
- Introduction to cybercrime
- Cybercrime investigation types overview
- Challenges in digital forensics and cybercrime
- Digital Evidence and the law (Country-specific)

### 4. People Domain: DF-C$^2$M$^2$ Personnel Capability Maturity Model, tools, assessments and development guidelines:

This provides the DF-C$^2$M$^2$ tools to implement for Personnel Capability Maturity. DF-C$^2$M$^2$ Personnel Capability Maturity, related process improvements, and the DF-C$^2$M$^2$ body of knowledge can help digital forensic laboratories assess and improve greater efficiency and customer satisfaction.

[4] http://www.ecru.co.uk/portfolio/gpen.html - as accessed 26 Dec 2012

**5. People & Process Domains: Proposed DF-C$^2$M$^2$ Digital Forensic Practitioner Licensing model:**

This provides the basis for testing, certification, and licensing of Digital Forensic Practitioners. This model was previously devised following extensive research as part of my MSc thesis, and the findings and requirements were integrated into the DF-C$^2$M$^2$ Body of Knowledge (following additional peer reviews and any further refinements that may be required). Implementation of the licensing model would be optional under the DF-C$^2$M$^2$, as this would be best implemented by regulatory authorities in the respective countries/legal jurisdictions.

**6. Process Domain: Quality Management requirements in line with ISO 17025 and ASCLD-LAB accreditation requirements**

This will be periodically reviewed and updated to help streamline the implementation of these standards and to implement any revisions to the standard. Updates would also provide accepted interpretations of the standards as they apply to digital forensic laboratories and operating environments. Future, planned ISO 27000 series digital forensic standards requirements will be more extensively integrated into the Quality Management System and related technical standard operating procedures as and when they become available as optional or elective components that labs may consider implementing.

**7. Process Domain: DF-C$^2$M$^2$ Six Steps Digital Forensic (case Lifecycle) Model**

The DF-C$^2$M$^2$ Six Steps model was developed as a hybrid model based on reviews of existing similar models, and based on what was believed to be more concise and suitable for implementation within their labs by the volunteer lab participants. All DF-C$^2$M$^2$ Body of knowledge Technical SOPs and procedures include and incorporate the elements of the DF-C$^2$M$^2$ Six Steps Model in their design and workflow.

**8. Process Domains - DF-C$^2$M$^2$ Case Audit requirements for cases.**

As part of the Quality Assurance element and a key element of the DF-C$^2$M$^2$ Quality Management System, these include detailed processes for technical (peer review) and procedural (administrative review) audits of all cases, including checklists, remediation guidelines, verification of evidence, and suitability of reports issued based on the DF-C$^2$M$^2$ Code of Conduct and minimum reporting requirements.

**9. Process Domain: DF-C$^2$M$^2$ Management System Audit planning and assessment guidelines**

This includes a DF-C$^2$M$^2$ (end to end) Audit Plan, and technical witness checklists and guidelines for technical assessments in preparation for ISO 17025/ASCLD-LAB audits and assessments.

**10. People, Processes & Tools Domains: DF-C$^2$M$^2$ Service Catalogue**

A catalogue of the most common and typical offerings (over 51 services) provided by the digital forensics lab details requirements, service planning requirements, limitations of the service, service planning guide, and related Service Level Target model covering the range of services defined within the DF-C$^2$M$^2$ Service Catalogue.

**11. Process Domain: DF-C$^2$M$^2$ Customer Service Satisfaction Tools.**

DF-C$^2$M$^2$ forms, tools, checklists, and guidelines for measuring and improving customer satisfaction for all digital forensic lab customers with provisions and guidelines for better managing and re-mediating customer complaints and low satisfaction ratings.

**12. Process and Tools Domains: DF-C$^2$M$^2$ Technical, Quality, and Management Best Practices:**

Digital technical and management best practice guidelines (technical manual workflows, forms, and guides).

All element of DF-C$^2$M$^2$ were reviewed by senior participants from participating labs in detail and per the evaluation process and participatory design process covered in Chapter 3 and 4. More participants would have allowed for broader input and feedback on these element, and perhaps would have altered some aspects of the model and its elements to some degree.

In addition to the technical and procedural workflow, the DF-C$^2$M$^2$ Body of Knowledge provides a complete set of ISO 17025/ASCLD-LAB compliant documentation forms, and guides to enable an existing or new lab to be able to quickly implement and update their existing processes in line with the requirements of DF-C$^2$M$^2$ in a relatively cost-effective manner [5] and still have the added benefit of incorporating Capability Maturity processes, tools, and guides to assist them in being able to measure/assess their capability maturity levels, and plan a roadmap to improve their overall Capability Maturity posture. Sample DF-C$^2$M$^2$ Process (SOPs) workflows are included in Appendix F.

Where applicable, the Body of Knowledge and the Assessment tool incorporate the Six Steps Model, and as can be seen from the sample Body of Knowledge workflow, with the Six Steps model elements highlighted in Figure 15.

The workflows and processes created in the Body of Knowledge are designed to create a best practice framework that can be readily adapted and implemented by digital forensic labs involved in digital evidence artefact examination and reporting, and these workflows and processes can be tailored to suit specific organisational requirements relatively easily. At a minimum these processes and workflows create a baseline which organisations may choose to build upon and tailor as may be required.

Labs that have relatively immature or ad-hoc processes and workflows could easily implement these workflows and procedures with minor customisations and have a relatively comprehensive set of policies and procedure in place in a short amount of time using the body of knowledge.

[5] Cost effective i.e. without the additional time and monetary investment in creating and designing new processes, forms and workflows,

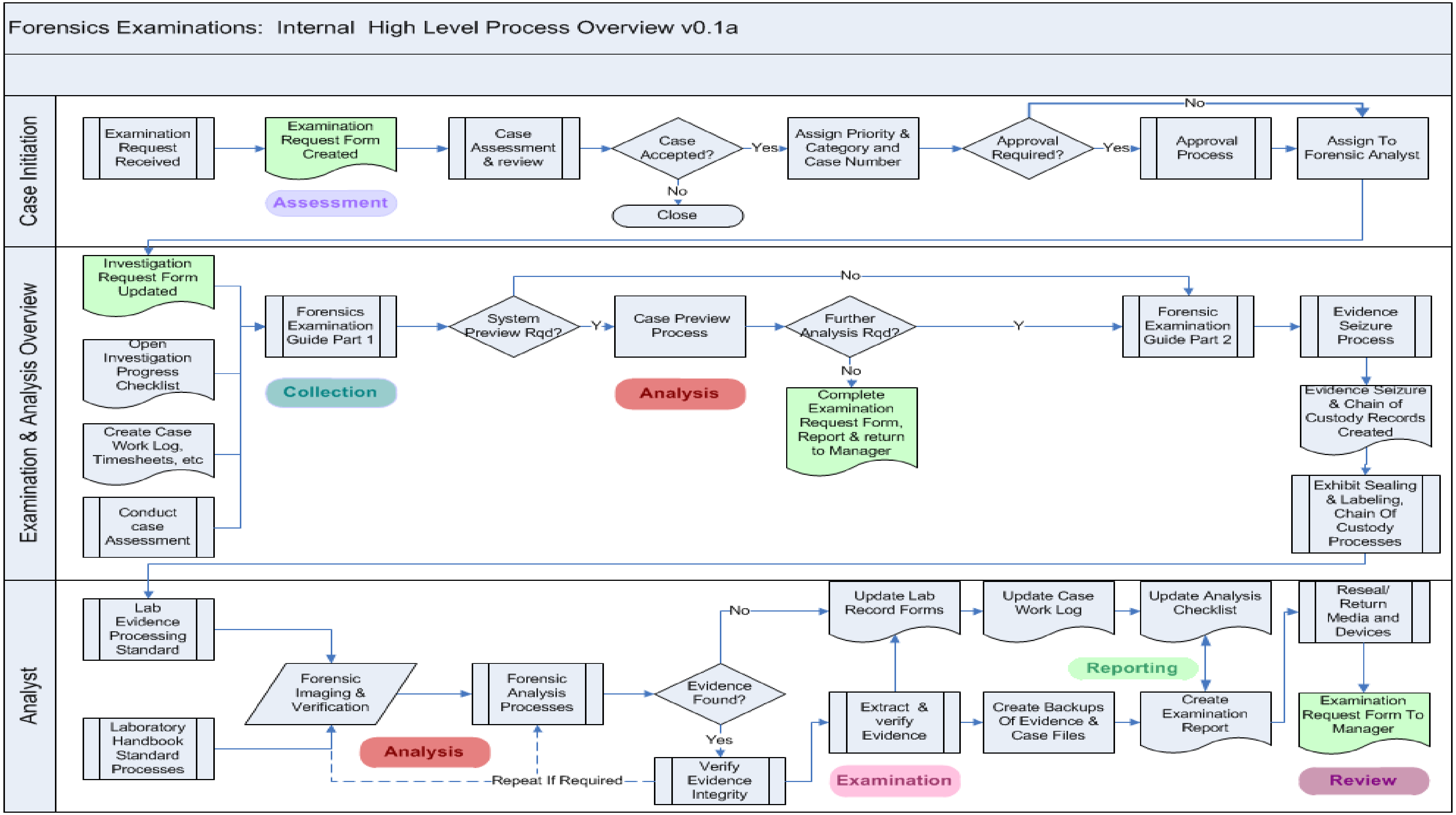

Forensics Examinations: Internal High Level Process Overview v0.1a
Case Initiation
Examination Request Received
Examination Request Form Created
Assessment
Case Assessment & review
Case Accepted?
Yes
No
Close
Assign Priority & Category and Case Number
Approval Required?
Yes
No
Approval Process
Assign To Forensic Analyst
Examination & Analysis Overview
Investigation Request Form Updated
Open Investigation Progress Checklist
Create Case Work Log, Timesheets, etc
Conduct case Assessment
Forensics Examination Guide Part 1
Collection
System Preview Rqd?
Y
No
Case Preview Process
Analysis
Further Analysis Rqd?
Y
No
Complete Examination Request Form, Report & return to Manager
Forensic Examination Guide Part 2
Evidence Seizure Process
Evidence Seizure & Chain of Custody Records Created
Exhibit Sealing & Labeling, Chain Of Custody Processes
Analyst
Lab Evidence Processing Standard
Laboratory Handbook Standard Processes
Forensic Imaging & Verification
Analysis
Forensic Analysis Processes
Repeat If Required
Evidence Found?
No
Yes
Verify Evidence Integrity
Update Lab Record Forms
Extract & verify Evidence
Examination
Update Case Work Log
Create Backups Of Evidence & Case Files
Update Analysis Checklist
Reporting
Create Examination Report
Reseal/ Return Media and Devices
Examination Request Form To Manager
Review

Figure 15: Relating the DF-C$^2$M$^2$ six steps digital forensic (case Lifecycle) model to the DF-C$^2$M$^2$ laboratory process overview

## 6.2 ASSESSING DIGITAL FORENSICS CAPABILITY MATURITY VIA THE DF-C$^2$M$^2$ ASSESSMENT TOOL

The DF-C$^2$M$^2$ Assessment tool is essentially a custom set of subject-specific spreadsheets, checklists, audit criteria, and skill assessment ratings. The DF-C$^2$M$^2$ assessment and evaluation tool was designed to allow an organisation and/or accrediting body to assess an organisation's compliance with the proposed DF-C$^2$M$^2$ requirements and to determine gaps and areas for improvement.

The overall output of the DF-C$^2$M$^2$ Assessment and Evaluation tool could also be used to benchmark various similar organisational entities, e.g. law enforcement digital forensic laboratories, against each other to determine:

- An industry baseline for digital forensics labs.
- A national benchmark.
- A roadmap to compliance with the DF-C$^2$M$^2$ requirements.
- A roadmap for ISO 17025/ASCLD/LAB accreditation.
- A means to measure Capability Maturity and People Capability Maturity within a given lab.

Additionally, specific assessment results can be considered for any of the three core components or their sub-domains, e.g. Personnel can be used to create a set of minimal requirements for licensing of personnel as licensed digital forensic practitioners in a specific area, and to provide a method for step-wise refinement and improvement of any of the sub-domains for both existing and newly formed digital forensic labs.

The key issues identified in Chapters 1 and 2, and the DF-C$^2$M$^2$ design elements highlighted in Chapter 5, inspired the creation of the DF-C$^2$M$^2$ Assessment Tools, the DF-C$^2$M$^2$ Framework, and DF-C$^2$M$^2$ Body of Knowledge. The DF-C$^2$M$^2$ Assessment and Planning tool which was initially created to assist in determining the capability maturity statues of participating labs, later proved to be an invaluable output of this research and a key component included in the Body of Knowledge based on participant feedback.

The DF-C$^2$M$^2$ assessment and planning tool provides a series of menus and flash screens within the tool to enable an assessor or manager to systematically navigate through the DF-C$^2$M$^2$ requirements based on organisation type, i.e. law enforcement (LE) or non-LE organisation, each of which may have slightly different requirements for a particular area such as personnel certification, etc. as detailed in Chapter 5.

The key elements of the DF-C$^2$M$^2$ assessment/planning tool are aligned with the three key domains of the DF-C$^2$M$^2$ (People, Processes, and Tools) and the key elements of each as described in Chapter 5.

The DF-C$^2$M$^2$ assessment and planning tool includes the following DF-C$^2$M$^2$ key management decision support and assessment tools:

1. The DF-C$^2$M$^2$ Service Catalogue.

2. The DF-C$^2$M$^2$ Process Requirements (based on organisation type, i.e. Law Enforcement or Non-Law Enforcement).

3. The DF-C$^2$M$^2$ Processes Capability Maturity assessment.

4. The DF-C$^2$M$^2$ People Requirements.

5. The DF-C$^2$M$^2$ Tools Requirements.

6. Overall DF-C$^2$M$^2$ Capability Maturity assessment.

7. DF-C$^2$M$^2$ Forensic Readiness Assessment (based on Six Steps Model).

8. Overall Lab Ratings.

**Note:** Each section within the tool includes the relevant Capability Maturity rating criteria as and where applicable.

## 6.3 THE DF-C$^2$M$^2$ ASSESSMENT TOOL

The DF-C$^2$M$^2$ Assessment Tool began as an audit checklist to be used to gather information across the three domains at the early stages of this research. Since then, the planning tool has evolved to be a dual-purpose planning and audit/assessment tool covering the various key aspects of a digital forensic lab.

The Assessment Tool draws from the Body of Knowledge for the various assessment criteria, and therefore is also categorised based on the three key domains – People, Processes, and Tools, as demonstrated in the review of the Assessment Tool in Sections 6.5, 6.6, and 6.7 of this chapter.

### 6.3.1 Introducing the DF-C$^2$M$^2$ Assessment and Planning Tool

The beta version of the tool is implemented as an Excel workbook containing 54 unique spreadsheets, graphs, and matrices at present. The tool is designed to be used as a standalone audit/assessment tool, and as part of the complete DF-C$^2$M$^2$ framework as a management decision support tool. It is perhaps, a more comprehensive ISO 17025-complaint digital forensics audit, assessment, and planning tool than other options presently available.

The modular design of the DF-C$^2$M$^2$ and the assessment tool means that additional requirements such as regulatory requirements can be added quite easily to the assessment and planning tool and be included in the overall assessment findings and ratings.

The assessment tool is closely linked with the Six Steps Model, and the assessment tool includes over 100 criteria mapped to the Six Steps Model, as listed in Chapter 5.

**Note:** Although it was decided based on previous experience earlier and on practitioner feedback during the workshops that the three DF-C$^2$M$^2$ domains all feed into and affect the Organisation (organisational issues), and that therefore there was no need to explicitly include ‘Organisation’ as a fourth domain, certain criteria included within the DF-C$^2$M$^2$ Organisation type are specific as explained in Chapter 5, and therefore the first section of the tool requests the user to select their organisation type, as shown in Figure 16.

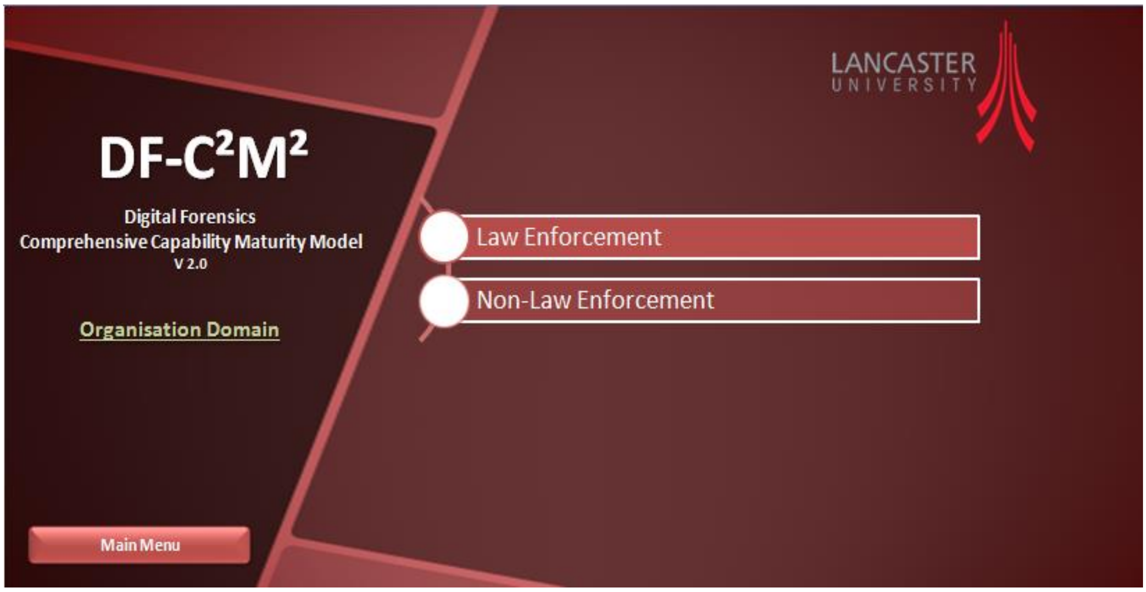


Figure 16: DF-C$^2$M$^2$ Tool - organisation type - start menu

For each organisation type, the following DF-C$^2$M$^2$ requirements are defined:

- DF-C$^2$M$^2$ Service Catalogue (covers requirements for People, Tools, and Processes)
- DF-C$^2$M$^2$ Forensic Readiness Assessment (People, Processes, and Tools requirements)
- ISO 17025 Assessment Results summary for addressing the DF-C$^2$M$^2$ digital forensics organisational maturity requirements
- People, Process and Tool Capability Maturity Ratings and checklists

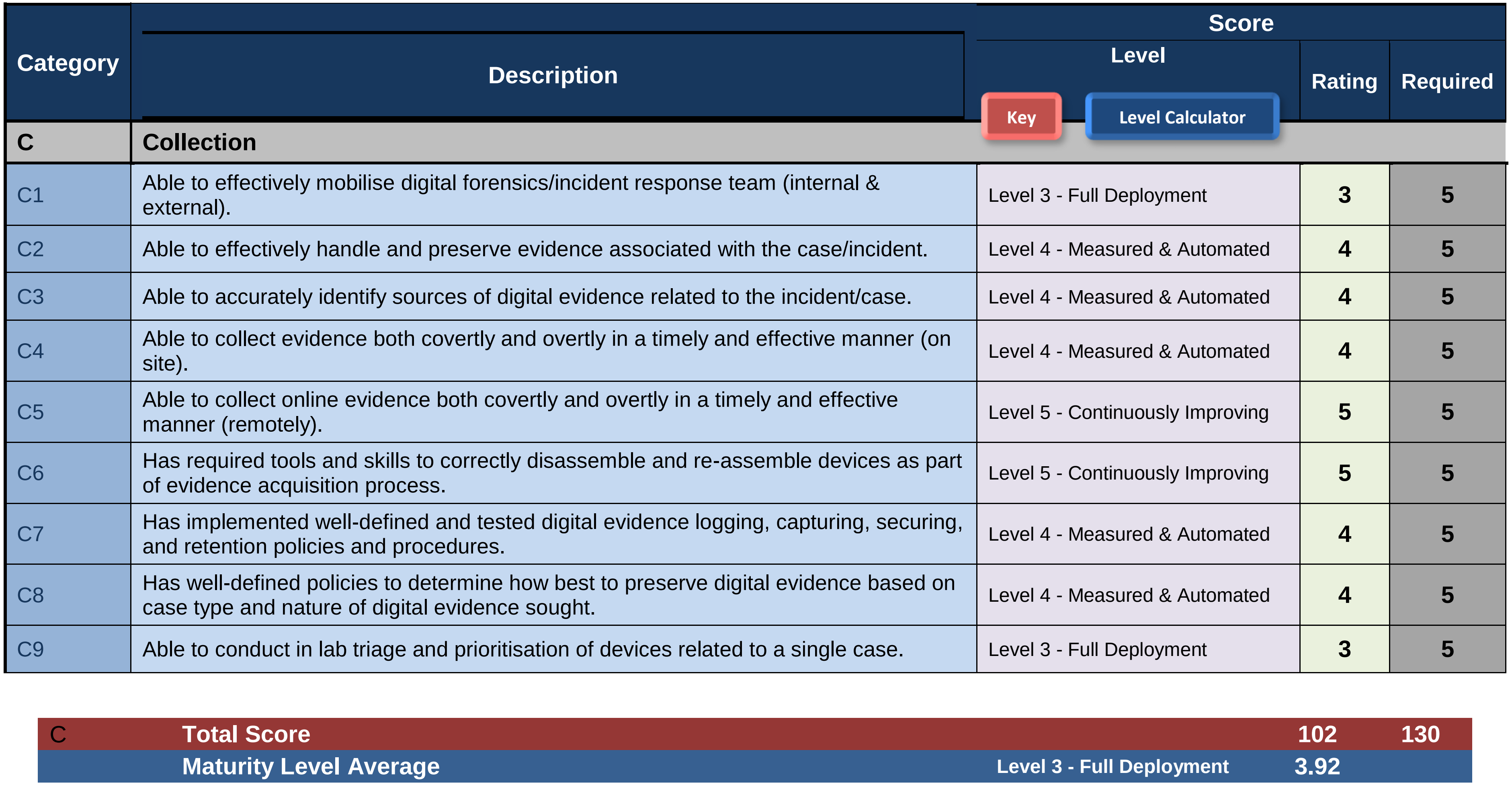
The DF-C$^2$M$^2$ Forensic Readiness Assessment covers the DF-C$^2$M$^2$ Six Steps Model, which includes the six essential key steps and elements of digital forensic analysis as viewed by the researcher, and as discussed in Chapter 5.

The DF-C$^2$M$^2$ Assessment and Planning tool extract below shows the assessment and development criteria required within the Process domain for one of the key elements in the six steps forensic process model – Collection as per the sample below, where 'Level' refers to the Capability Maturity Ratings for each of the criteria listed and is calculated based on users' input rating for a given criterion/line item.

In order to make the various criteria being assessed more objective rather than subjective, the user is able to expand each line item and receive additional hints (prompts or questions) to help qualify their rating and to guide them in more accurately reflecting the compliance level for each of the criteria.

Additionally, in the absence of an established benchmark rating for each criterion, the DF-C$^2$M$^2$ required rating score is included as a goal upon which prospective labs can aspire to achieve and therefore also help to achieve capability maturity for the area being assessed. Table 15 illustrates assessment tool criteria to evaluate for the Collection stage of the Six Steps Process Model with Criteria, Rating, and resulting Capability Maturity Rating for each of the criteria for this sub-element.

Table 15: Sample extracts of LE readiness assessment criteria



| Category | Description | Score | | |
|---|---|---|---|---|
| | | Level<br>Key<br>Level Calculator | Rating | Required |
| C | Collection | | | |
| C1 | Able to effectively mobilise digital forensics/incident response team (internal & external). | Level 3 - Full Deployment | 3 | 5 |
| C2 | Able to effectively handle and preserve evidence associated with the case/incident. | Level 4 - Measured & Automated | 4 | 5 |
| C3 | Able to accurately identify sources of digital evidence related to the incident/case. | Level 4 - Measured & Automated | 4 | 5 |
| C4 | Able to collect evidence both covertly and overtly in a timely and effective manner (on site). | Level 4 - Measured & Automated | 4 | 5 |
| C5 | Able to collect online evidence both covertly and overtly in a timely and effective manner (remotely). | Level 5 - Continuously Improving | 5 | 5 |
| C6 | Has required tools and skills to correctly disassemble and re-assemble devices as part of evidence acquisition process. | Level 5 - Continuously Improving | 5 | 5 |
| C7 | Has implemented well-defined and tested digital evidence logging, capturing, securing, and retention policies and procedures. | Level 4 - Measured & Automated | 4 | 5 |
| C8 | Has well-defined policies to determine how best to preserve digital evidence based on case type and nature of digital evidence sought. | Level 4 - Measured & Automated | 4 | 5 |
| C9 | Able to conduct in lab triage and prioritisation of devices related to a single case. | Level 3 - Full Deployment | 3 | 5 |

| | | | | |
|---|---|---|---|---|
| C | Total Score | | 102 | 130 |
| | Maturity Level Average | Level 3 - Full Deployment | 3.92 | |

Additionally, a total score and Maturity Level Rating are calculated for each overall section assessed, as shown above.

Additionally, in order to help address the challenges related to the creation of policies, processes, and forms for each section (required under ISO 17025), the DF-C$^2$M$^2$ assessment tool refers the assessor to the DF-C$^2$M$^2$ Body of Knowledge relevant section (document, form, or policy) that addresses each item being assessed (prescriptive information), thus enabling quick and easy process-corrective actions to be undertaken.

This single feature is perhaps one of the most valuable features to enable labs to quickly develop and/or re-mediate issues related to lack of or inadequate policies, processes, workflows, and forms. This prescriptive or re-mediation feature enables a newly established digital forensic lab, for example, to quickly develop their internal documentation (People, Processes, and Tools) manuals, forms, workflows, and controls by simply customising the existing collateral within the Body of Knowledge, thus helping to reduce the need for the timely and often costly initial establishment of ISO 17025 policies and procedures.

Whereas most projects to establish ISO 17025 complaint policies and procedures for a digital forensic lab may take up to 6 - 18 months to achieve, the DF-C$^2$M$^2$ Body of Knowledge would enable a lab to achieve the same within an estimated third of the time, and possibly without the need to involve external third-party consultants, thus helping to address issues related to the cost of ISO 17025 initial implementation, and the amount of time required to allow a newly established lab to become operational under ISO 17025 criteria.

Sample training material for personnel on ISO 17025 and the DF-C$^2$M$^2$ policies, procedures, and workflows is also included with sample personnel quizzes and tests.

### 6.3.2 Key Maturity Levels

For each DF-C$^2$M$^2$ requirement assessed, a maturity level is assigned based on a rating given by the assessor. These maturity levels and related criteria differ based on the nature of what is being assessed i.e. People, vs. Processes, vs. Tools, etc. Table 16 adapted from Srinivasan & Murthy' Maturity Level Snapshot (Srinivasan & Murthy) and Humphrey's CMM Levels (Humphrey W. , 1989) - provides a sample of the Process Maturity Ratings used for DF-C$^2$M$^2$ Process Assessments.

**Table 16: Process Maturity Ratings Matrix**

| | Assessor Criteria => | Person-Dependent (Ad-Hoc Processes) | Documented Processes Exist | Processes Partially Deployed | Processes Fully Deployed | Processes Measured & Automated | Continuously Improving |
|---|---|---|---|---|---|---|---|
| CMM Level (0 – 5) | Level 0 None | Yes | – | – | – | – | – |
| | Level 1 Initial | – | Yes | – | – | – | – |
| | Level 2 Managed | – | Yes | Yes | – | – | – |
| | Level 3 Defined | – | Yes | – | Yes | – | – |
| | Level 4 Qualitatively Managed | – | Yes | – | Yes | Yes | – |
| | Level 5 Optimising | – | Yes | – | Yes | Yes | Yes |

The Process Maturity Ratings Matrix enables an assessor to determine the CMM of the organisation being assessed for example if the organisation's processes are partially deployed, the maximum CMM rating the organisation could obtain would be Level 2. If on the other hand documented processes exist, then the level of deployment/implementation should then be considered. The possible levels of implementation deployment are partially deployed, fully deployed, Measured and Automated, and Continuously Improving.

Deployment level and whether these processes are meet the CMM definitions of either Initial, Managed, Defined, Qualitatively Managed or optimising as per CMM standard categories (Curtis, Hefley, & Miller, 2002)

If an organisation's digital forensics processes were fully implemented, they may qualify for CMM rating of Level 3, 4 or 5 depending on other criteria determined within the assessment tool.

## 6.4 CONDUCTING THE READINESS ASSESSMENT

The readiness assessment is a key part of DF-C²M² as an assessment, planning and audit tool. For each of the DF-C²M² requirements (assessment criteria), the assessor is guided within the tool with pointers. Prompts help them to assess a variety of subjective criteria, including fundamental CMM criteria such as:

1. Is the process/task currently being performed?
2. Is the process/task documented?
3. Is the process/task well-understood by those responsible for ensuring compliance/performing the task?
4. Is the process/task auditable/verifiable? If not, can it be demonstrated and witnessed?
5. Under what circumstances have deviations from the documented process occurred? How were these documented? Authorised? What corrective actions were taken to reduce the likelihood of repeated deviations?
6. Identify gaps and areas for improvement

Figure 17 illustrates the assessment tool components and structure. In addition, the assessor should also factor in Maturity level ratings (used in the DF-C²M² assessment tool) as per Table 17 shown as presented by Srinivasan and Murthy (Srinivasan & Murthy).

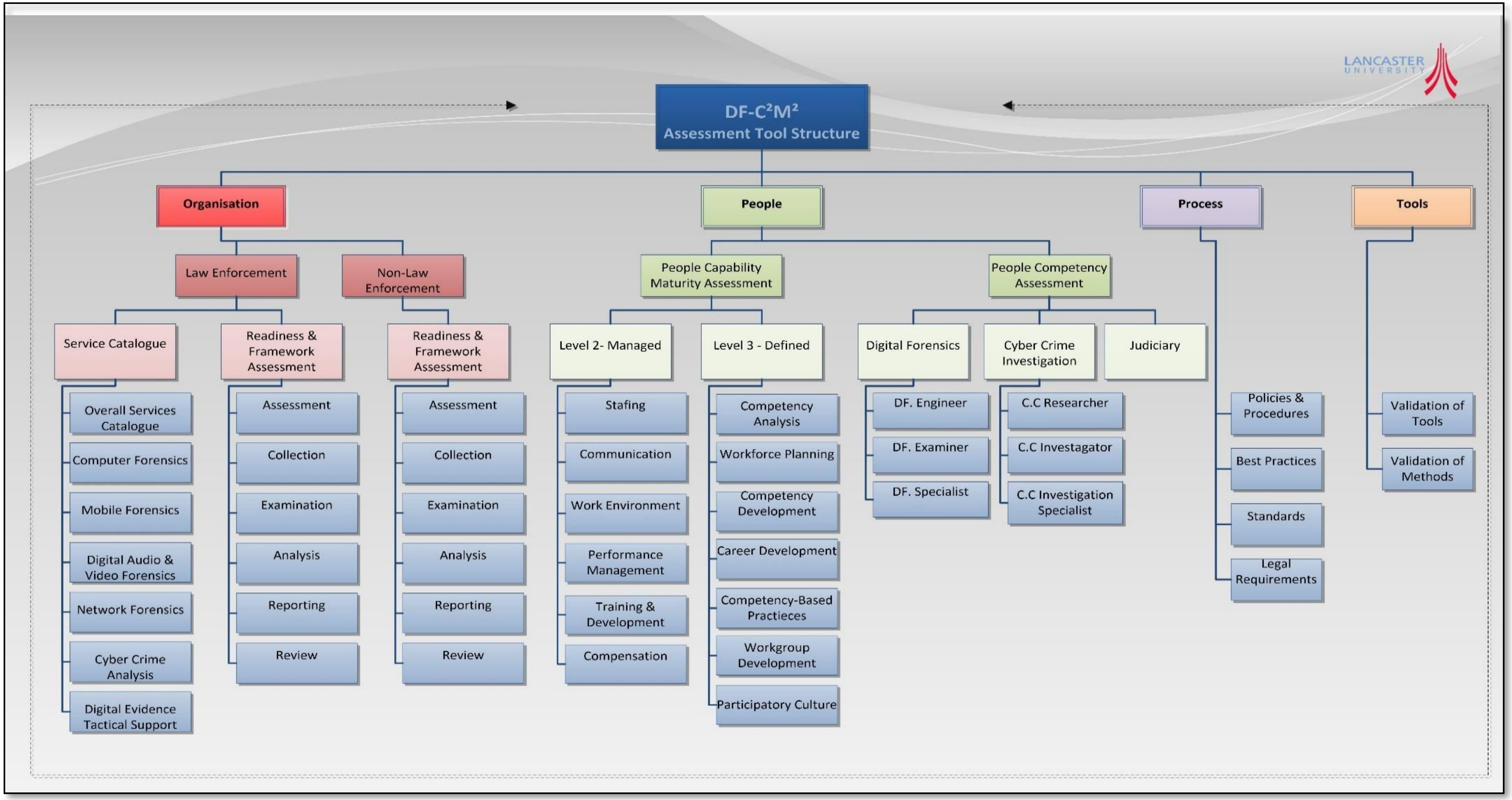


Figure 17: DF-C²M² assessment tool structure

Table 17: Process maturity level guide (Srinivasan & Murthy)

**Level 0 – Person-Dependent Practices:** This is for cases where the activity being performed is not documented. In other words, it is not recorded either in outline or in detail. The activity is entirely person-dependent and the sequence, timing, and result may vary during repetition. This requires a lot of supervision. There is no guarantee of either achieving the desired result or adhering to timelines. The activity is entirely ad hoc, with little communication between functions. The effectiveness of the activity is entirely dependent on individuals. Knowledge transfer may or may not happen if there is any change in the owner of the activity.

**Level 1 – Documented Process:** At this maturity level, there is a document that has been reviewed and approved by the supervisor or the approving authority as the standard process. However, it may be doubtful that the activity being performed is as per the document. This is may be because of a process drift or some drastic change since the document was drafted.

**Level 2 – Partial Deployment:** Here, the activity that is documented is being deployed, but there is inconsistency in the deployment. The process may not be deployed in totality. That is, it may not be deployed at all the intended locations, or though all functions, or by all of the intended owners, or all of the activities defined in the process are not being performed. This would mean that the document has not been designed to cater to such variations. There is inconsistency in the results of different process owners.

**Level 3 – Full Deployment:** At this level, there is no inconsistency between the documented process and the deployed process. The process documented and deployed caters to all of the intended locations, owners, and activities that need to be performed. The process also shows seamless linkage between functions and other processes wherever there needs to be any interaction. This means that the process shows greater consistency of actions and better communication between functions.

**Level 4 – Measured and Automated:** The process has set itself goals such as adherence to timelines, customer satisfaction, cost, etc. The process is also being measured against its goals. The process is system-driven by enablers such as using enterprise resource planning, customer resource management, or any other custom-made software.

**Level 5 – Continuously Improving:** The goals set for the process are being analysed for achievements and improved regularly. The timelines, cost targets, and satisfaction levels are being achieved regularly, and the targets are also being tightened by using continuous quality improvement techniques such as Six Sigma, Kaizan, etc. The enabling system is also being improved and being made error-free by strategies such as mistake proofing.

In addressing the need to be able to assess gaps within an organisation as mentioned in Chapters 1 and 5, the assessment tool should be applied by both newly established digital forensic laboratories and by established digital forensic laboratories that are keen to improve their overall efficiency and capability maturity in the three key domains covered in this model.

Figure 18 shows a snapshot dashboard result of a sample assessment that, at a glance, can provide management with a summary of areas that need improvement for each of the three key domains, and overall maturity level based on the DF-C²M² criteria.

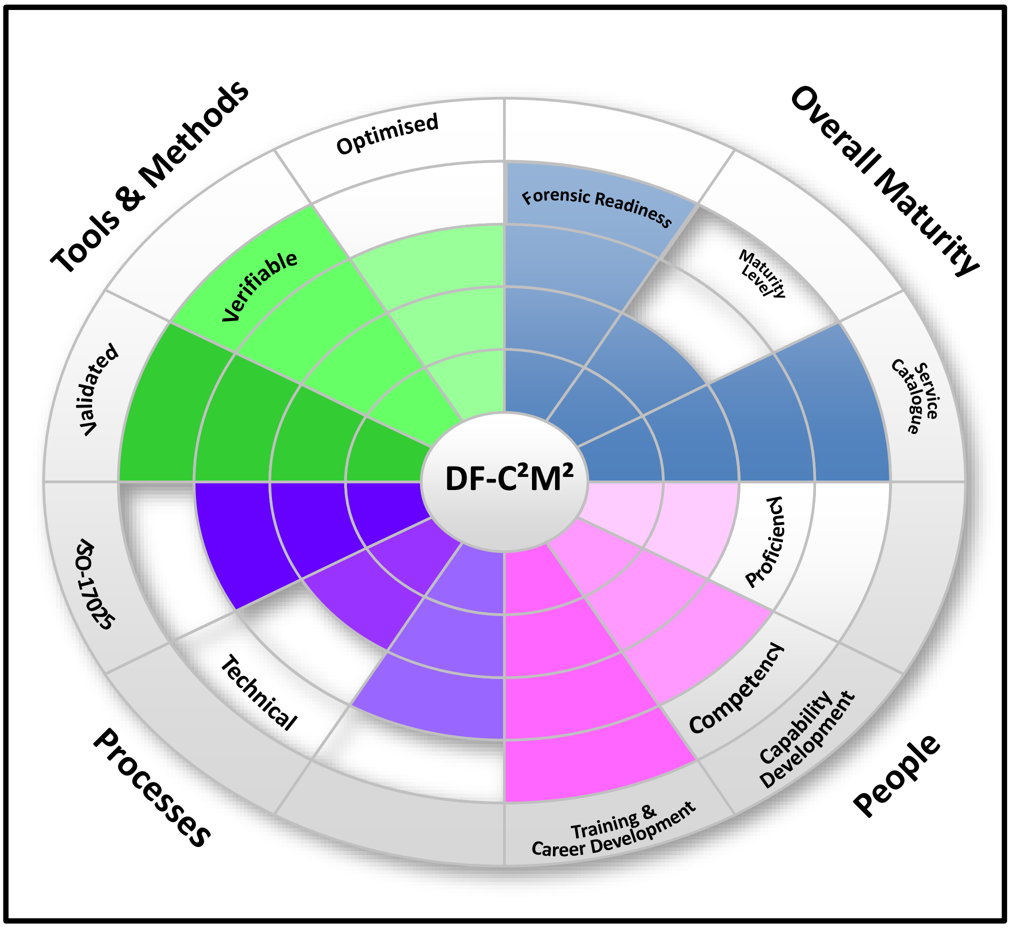


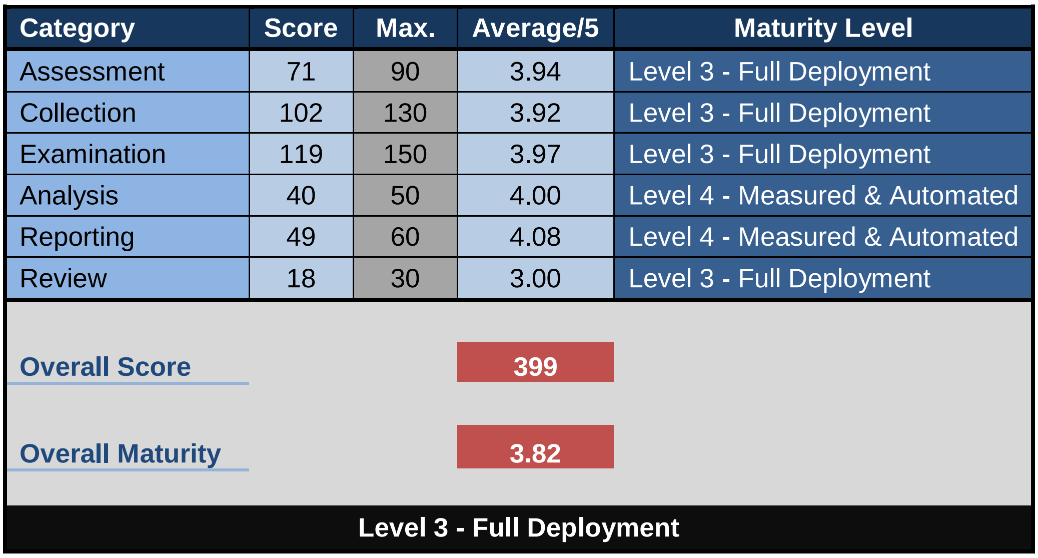
**Figure 18: Sample DF-C²M² assessment/compliance results dashboard**

Figure 18 shows CMM levels for People (Pinks), Process (Purples) and Tools (Greens) and an Overall Maturity (Blue) rating for a given organisation. Starting from the core with CMM rating of 1, this dashboard shows incremental blocks for each additional CMM level achieved. For example, in the above example Training & Career development is rated as 5, whilst Competency is rated as 4, and Proficiency is rated 3.

During evaluation and feedback of the DF-C$^2$M$^2$, participants indicated that this (dashboard result above) was potentially one of the most useful results produced by the assessment tool, providing management with the summary information they need when looking at where their lab is versus where it wants to be in terms of compliance and maturity. Other sample assessment results produced by the DF-C$^2$M$^2$ assessment tool include:

**1. Sample Six Steps Process Model (Forensic Readiness) Assessment Result (Table 18):**

Table 18: DF-C$^2$M$^2$ Tool: maturity level assessment



| Category | Score | Max. | Average/5 | Maturity Level |
|---|---|---|---|---|
| Assessment | 71 | 90 | 3.94 | Level 3 - Full Deployment |
| Collection | 102 | 130 | 3.92 | Level 3 - Full Deployment |
| Examination | 119 | 150 | 3.97 | Level 3 - Full Deployment |
| Analysis | 40 | 50 | 4.00 | Level 4 - Measured & Automated |
| Reporting | 49 | 60 | 4.08 | Level 4 - Measured & Automated |
| Review | 18 | 30 | 3.00 | Level 3 - Full Deployment |
| Overall Score | | | 399 | |
| Overall Maturity | | | 3.82 | |
| Level 3 - Full Deployment | | | | |

**2. Sample readiness assessment results with DF-C$^2$M$^2$ Current Six Steps Model Ratings vs. Goal (Figure 19):**

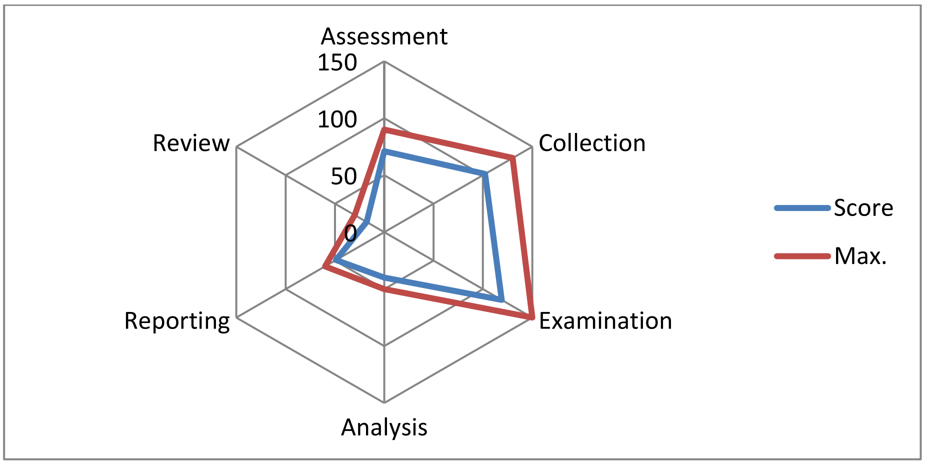


Figure 19: DF-C$^2$M$^2$ Tool: readiness assessment results – six Steps process model - current vs. required

3. **Assessment results vs. proposed DF-C²M² sample benchmark result (Figure 20):**

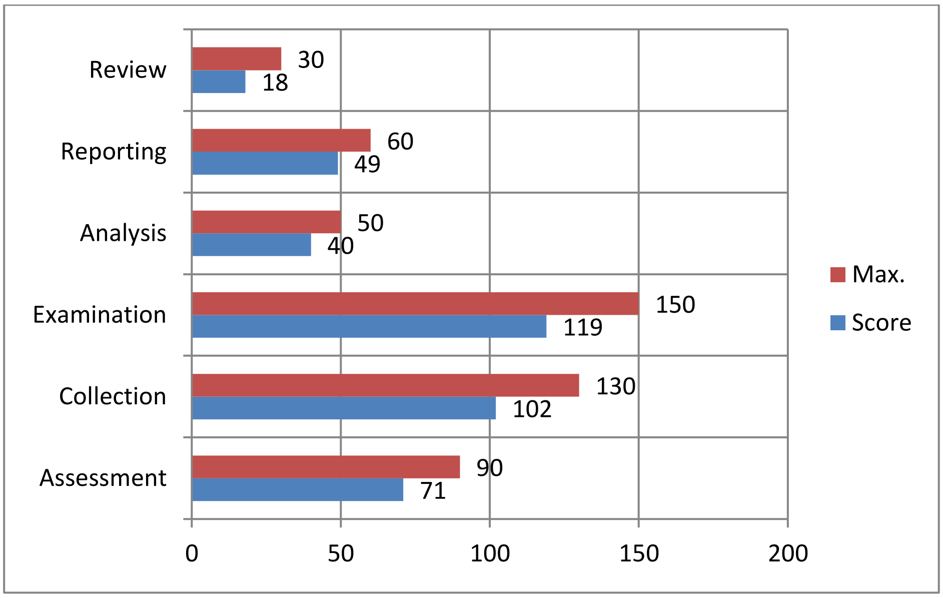


**Figure 20: DF-C²M² Tool: readiness assessment – Six Steps process rating vs. assumed industry benchmark**

### 6.4.1 DF-C²M² and Achieving ISO 17025 Accreditation

As was noted in Chapter 1, accreditation was a key requirement for the majority of digital forensic laboratories, and in many instances complying with accreditation requirements was a primary issue, while achieving capability maturity was cited as a lesser priority amongst lab personnel interviewed, but as an equally important priority amongst the Lab Managers interviewed.

By design, the DF-C²M² addresses the key areas of ISO 17025 accreditation requirements coupled via the inclusion of ISO 17025 specific audit and assessment requirements, and ASCLD-LAB supplemental requirements.

## 6.5 DF-C²M² PEOPLE DOMAIN - ASSESSMENT TOOL

Perhaps the most novel aspect of this research is the application of People Capability Maturity (P-CMM) and Process Capability Maturity (CMM) to the specialist field of digital forensics. As cited in Chapter 1, many labs are faced with the need to reduce backlogs and improve efficiency with little or no reference framework on how to assess their current effectiveness and plan a way forward. (Goodison, Davis, & Jackson, 2014).

The inclusion of P-CMM and CMM within the model enables managers to assess whether delays are mostly due to the nature of the cases, the volume of data, or the effectiveness of their processes and personnel, i.e. Capability Maturity.

To address the Capability Maturity requirements of the DF-C²M², the People domain of the DF-C²M² and the DF-C²M² Assessment tool explicitly cover two specific areas, namely Competency of Personnel and People Capability Maturity as discussed in Chapter 5, and as cited as issues in Chapter 1. Competency within the DF-C²M² and Assessment tool applies to the following three related areas covered within the DF-C²M²:

1. Competency of Digital Forensics Personnel (based on job roles).
2. Competency of Cybercrime Personnel (based on job roles).
3. Competency of Judiciary (related to Digital Forensics and Cybercrime awareness).

Each of these will be discussed in further detail in the sections below.

### 6.5.1 Assessing Competency of Digital Forensics Personnel

Within the specialist area of Digital Forensics, five specific technical job roles have been identified and job descriptions drafted for use within the DF-C²M². These five technical roles defined within the DF-C²M² are:

- Digital Forensic Trainee
- Digital Forensic Engineer
- Digital Forensic Examiner
- Senior Digital Forensic Examiner
- Digital Forensic Specialist

The requirements for each role were identified during the investigation stage of this research, were based on a proposed model that would work equally well in small to large digital forensic laboratories and could easily be adapted for existing laboratories based on practitioner feedback as discussed in Chapters 3 and 4.

Within the DF-C$^2$M$^2$ assessment, the training requirements for the role of Digital Forensic Engineer or Digital Forensic Examiner, for example, includes the following key areas of knowledge and competency test areas. Table 19 shows sample competency test criteria for Digital Forensic Examiners:

**Table 19: Digital forensic engineer and examiner competency test areas**

| |
|---|
| IT Fundamentals |
| Forensics Introduction |
| Forensics Fundamentals |
| Mobile Forensics |
| Primary Forensic Tools |
| Operating Systems - Technical |
| Lab Processes |
| Soft Skills |

Each of these areas is assessed using a combination of written tests, practical demonstrations (witnessing tests), lab-related documentation, and reviews of previous case work as part of the assessment tool implementation.

Within the Model and therefore the Assessment tool, the Digital Forensic Examiner requirements and levels of competency are naturally higher than those of an Engineer as determined during the participant feedback of requirements during the research. Additionally, each of the eight areas above contain more criteria for Digital Forensic Examiners in comparison with the requirements for Digital Forensics Engineers. Table 20 shows sample competency test criteria for Digital Forensic Examiners.

**Table 20: DF-C$^2$M$^2$ sample competency test criteria for digital forensic examiners**

| | | | Skill Level | Score | Required | Max. |
|---|---|---|---|---|---|---|
| IT Fundamentals | 1 | Computer Fundamentals (A+) | Level 2 - Beginner | 2 | 4 | 5 |
| | 2 | Network Fundamentals (Network+) | Level 1 - Novice | 1 | 4 | 5 |
| | 3 | Security Fundamentals (Security+) | Level 4 - Proficient | 4 | 4 | 5 |
| Forensics Introduction | 4 | ISO 27037 (Forensics Responder) & APCO Digital Forensic Principles | Level 2 - Beginner | 2 | 4 | 5 |
| | 5 | Media Wiping & Verification | Level 2 - Beginner | 2 | 4 | 5 |
| | 6 | Media Imaging & Verification | Level 4 - Proficient | 4 | 4 | 5 |
| | 7 | Forensics Workstation Operation & Maintenance | Level 2 - Beginner | 2 | 4 | 5 |
| | 8 | Ghost Process & Rebuild (Verification) | Level 3 - Competent | 3 | 4 | 5 |
| | 9 | Media Imaging: Dossier Operation | Level 3 - Competent | 3 | 4 | 5 |
| | 10 | Media Imaging: Omniwipe Operation | Level 2 - Beginner | 2 | 4 | 5 |
| | 11 | Bulk Media Imaging: Rimage Operation | Level 2 - Beginner | 2 | 4 | 5 |
| | 12 | Write-Blocker Usage & Testing | Level 2 - Beginner | 2 | 4 | 5 |

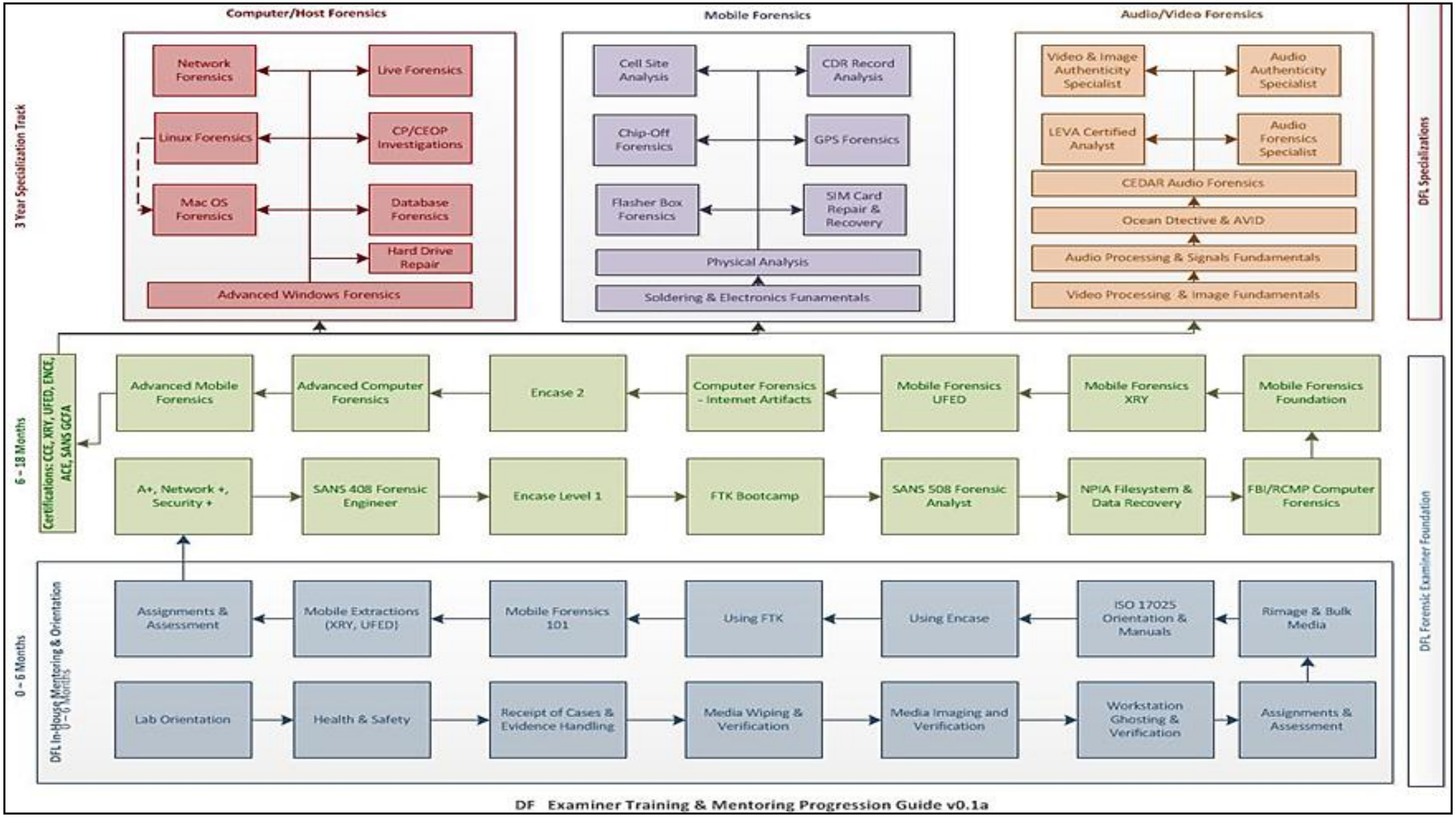
In contrast, as defined in Chapter 5, the DF-C²M² Digital Forensic Specialist Competency Testing is dependent on the Competency test areas for Digital Forensic Engineers and Examiners, but has significantly different specialist and advanced subjects included, as shown in Table 21:

**Table 21: DF-C²M² sample competency test criteria for digital forensic specialists**

| | | Skill Level | Score | Required | Max. |
|---|---|---|---|---|---|
| 1 | Forensic Engineer Rating | Level 3 - Competent | 3 | 4 | 5 |
| 2 | Forensic Examiner Rating | Level 2 - Beginner | 2 | 4 | 5 |
| 3 | Advanced Operating System Forensics | Level 4 - Proficient | 4 | 4 | 5 |
| 4 | Forensic Programming and Scripting (1 language) | Level 3 - Competent | 3 | 4 | 5 |
| 5 | Advanced Media Recovery & Repair | Level 4 - Proficient | 4 | 4 | 5 |
| 6 | Cybercrime Investigation | Level 3 - Competent | 3 | 4 | 5 |
| 7 | Information Security Specialisation | Level 2 - Beginner | 2 | 4 | 5 |
| 8 | Live Memory Analysis | Level 4 - Proficient | 4 | 4 | 5 |
| 9 | Network Forensics | Level 2 - Beginner | 2 | 4 | 5 |
| 10 | Advanced Linux Forensics | Level 3 - Competent | 3 | 4 | 5 |

**Note** that the Digital Forensics Specialisation, namely Computer Forensics, Mobile Device Forensics, and Digital Audio/Video Forensics, also have specialty sub-domains, and each has its own additional set of competency test criteria.

Within the implementation of the DF-C²M² Body of Knowledge are detailed training and career progression plans that include formal and on-the-job training requirements as defined within Chapter 5. Those personnel that already meet the required criteria based and qualifications and experience could opt to take competency assessment in each required area, and thus progress to the next stage or role within the lab relatively easily. Competency and proficiency testing for each technical role is based upon the established lab procedures, as well as the knowledge each candidate should possess based on their job role-specific training and career development plan in accordance with the requirements of ISO 17025. Figure 21 illustrates the DF-C²M² sample career development and training plan covering all roles from Digital Forensic Trainee through Digital Forensic Specialist:


Computer/Host Forensics
Network Forensics
Live Forensics
Linux Forensics
CP/CEOP Investigations
Mac OS Forensics
Database Forensics
Hard Drive Repair
Advanced Windows Forensics
Mobile Forensics
Cell Site Analysis
CDR Record Analysis
Chip-Off Forensics
GPS Forensics
Flasher Box Forensics
SIM Card Repair & Recovery
Physical Analysis
Soldering & Electronics Funamentals
Audio/Video Forensics
Video & Image Authenticity Specialist
Audio Authenticity Specialist
LEVA Certified Analyst
Audio Forensics Specialist
CEDAR Audio Forensics
Ocean Dtective & AVID
Audio Processing & Signals Fundamentals
Video Processing & Image Fundamentals
DFL Specializations
3 Year Specialization Track
6 – 18 Months
Certifications: CCE, XRY, UFED, ENCE, ACE, SANS GCFA
Advanced Mobile Forensics
Advanced Computer Forensics
Encase 2
Computer Forensics - Internet Artifacts
Mobile Forensics UFED
Mobile Forensics XRY
Mobile Forensics Foundation
A+, Network +, Security +
SANS 408 Forensic Engineer
Encase Level 1
FTK Bootcamp
SANS 508 Forensic Analyst
NPIA Filesystem & Data Recovery
FBI/RCMP Computer Forensics
DFL Forensic Examiner Foundation
0 – 6 Months
DFL In-House Mentoring & Orientation 0 – 6 Months
Assignments & Assessment
Mobile Extractions (XRY, UFED)
Mobile Forensics 101
Using FTK
Using Encase
ISO 17025 Orientation & Manuals
Rimage & Bulk Media
Lab Orientation
Health & Safety
Receipt of Cases & Evidence Handling
Media Wiping & Verification
Media Imaging and Verification
Workstation Ghosting & Verification
Assignments & Assessment
DF Examiner Training & Mentoring Progression Guide v0.1a

Note: Product specific may be taken in any order as long as the required course pre-requisites have been met, e.g.: FTK before Encase

Figure 21: DF-C²M² sample digital forensic training & career development progression plan

### 6.5.2 Assessing Competency of Cybercrime Investigation Personnel

Through the series of practitioner interviews conducted, it was determined through a job/role analysis exercise conducted as part the interviews; that digital forensic personnel were often required to also provide analysis of cybercrime-related artefacts, provide technical advice to investigation units, and assist with digital investigations for cybercrime-related cases.

Very little exists to assist with defining baseline processes, tools, methods, and People, Processes, and Tools requirements for effective cybercrime investigations. The roles of cybercrime investigations-related personnel were not well-defined across organisations, and therefore as a related digital forensic lab issue, cybercrime job roles and training career progression plans were created as part of the implementation of the DF-C$^2$M$^2$ Assessment tool and Body of Knowledge to help address this requirement cited as an overlooked yet essential requirement by some digital forensic practitioners.

The model was recently addressed in part by Kerrigan as reviewed in Chapter 2, but it was felt that insufficient detail was given to the three-key cybercrime-related areas addressed within the DF-C$^2$M$^2$, namely job roles, career development, and training plans, and competency testing based on the previous two areas.

Kerrigan’s Digital Investigations Capability Maturity Model (DI-CMM) (kerrigan, 2013) focusses on five generic groupings of tasks associated with digital investigations.

Thus, within the specialist area of cybercrime investigation, three specific technical job roles have been identified and job descriptions drafted for use within the DF-C$^2$M$^2$. These three technical roles defined within the DF-C$^2$M$^2$ are:

- Cybercrime Research Analyst
- Cybercrime Investigator
- Cybercrime Investigation Specialist

The requirements for each role were identified during the investigation stage of this research, are based on a proposed model that would work equally well in small to large organisations, and could easily be adapted for existing organisations.

In addition to a job description that defines the core functions and responsibilities of each of these technical roles, the DF-C$^2$M$^2$ also prescribes a proposed training and career progression path to allow entry-level personnel such as Cybercrime Research Analysts to progress to becoming Cybercrime Investigation Specialists, and then later become specialists.

The proposed career progression path covers a mixture of both on-the-job and formal training, and defines a suggested minimum working period for each of the roles before one can progress to the next level as defined within the design stage of the model (Chapter 5). Experienced candidates would be able to be fast tracked through levels, by simply demonstrating their knowledge of the processes and completing the relevant competency, proficiency and certification requirements for each role. Competency testing as well as external proficiency testing (of the personnel function in Examiner roles) is required, and overall cybercrime investigation unit proficiency tests are required to help assess the overall proficiency of the unit.

Within the DF-C$^2$M$^2$, the assessment and therefore training requirements for the role of Cybercrime Research Analyst or Cybercrime Investigator, for example, includes certain common areas of knowledge and competency.  DF-C$^2$M$^2$ Sample competency test criteria for Cybercrime Research Analysts are shown in Table 22.

**Table 22: DF-C$^2$M$^2$ sample competency test criteria for cybercrime research analysts**

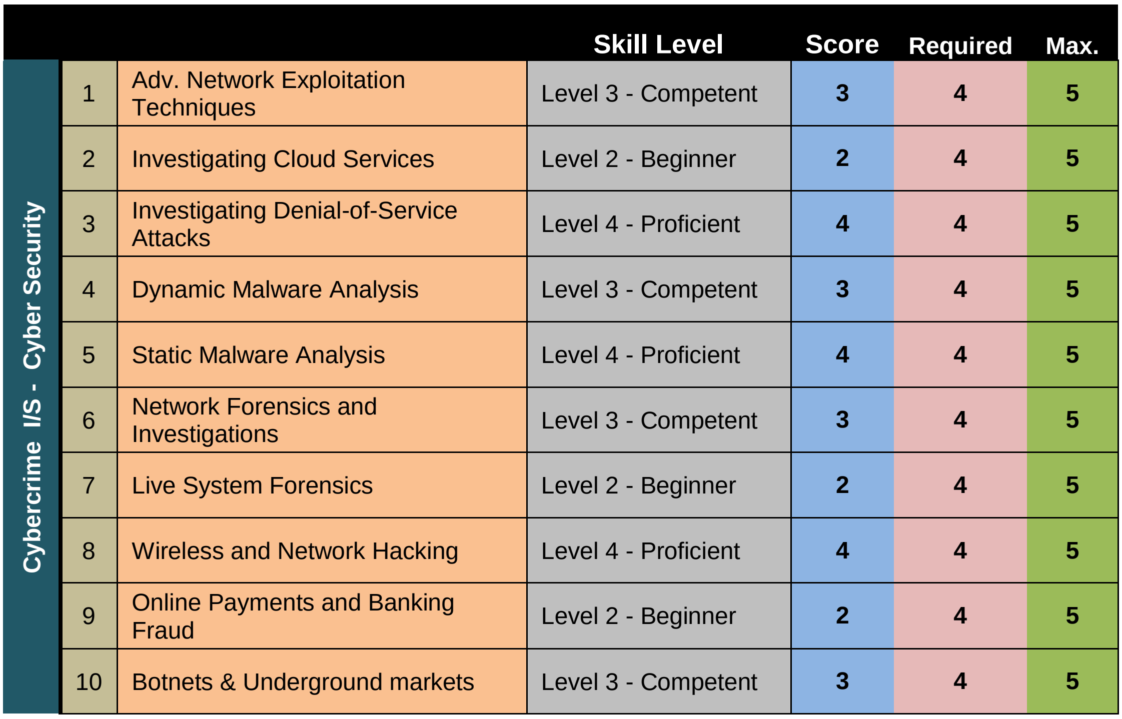
| | | Skill Level | Score | Required | Max. |
|---|---|---|---|---|---|
| 1 | Information Security Essentials (SANS GSEC & Security+) | Level 3 - Competent | 3 | 4 | 5 |
| 2 | Network Fundamentals (CCNA) | Level 2 - Beginner | 2 | 4 | 5 |
| 3 | Ethical Hacking 101 (CEH) | Level 4 - Proficient | 4 | 4 | 5 |
| 4 | Introduction to Internet Investigations | Level 3 - Competent | 3 | 4 | 5 |
| 5 | Introduction to Cyber & High-Tech Crimes | Level 4 - Proficient | 4 | 4 | 5 |
| 6 | Digital Evidence Identification, Handling & Seizure (ISO 27037) | Level 3 - Competent | 3 | 4 | 5 |
| 7 | Introduction to Credit Card Fraud & ATM Skimming | Level 2 - Beginner | 2 | 4 | 5 |
| 8 | Understanding Scams and 419 cases & Investigation Techniques | Level 4 - Proficient | 4 | 4 | 5 |
| 9 | Understanding Social Media | Level 2 - Beginner | 2 | 4 | 5 |
| 10 | Social Media Investigation Processes and Tools | Level 3 - Competent | 3 | 4 | 5 |
| 11 | Introduction to Open Source Intelligence | Level 2 - Beginner | 2 | 4 | 5 |

For Cybercrime Investigation Specialists, three areas of specialisation are defined; these are:

A. Cybercrime Investigations – Cyber Security.
B. Cybercrime Investigations – Covert.
C. Cybercrime Investigations – OSINT.

Each of these areas of specialisation has its own competency test criteria, e.g. Cybercrime Investigations – Cyber Security, Covert Investigations, Open Source Intelligence, etc. Table 23 presents a sample of specialisation criteria used in the assessment tool for the position of Cybercrime Investigator:

Table 23: DF-C²M² cybercrime investigations – cyber security investigations



| | | | Skill Level | Score | Required | Max. |
|---|---|---|---|---|---|---|
| Cybercrime I/S - Cyber Security | 1 | Adv. Network Exploitation Techniques | Level 3 - Competent | 3 | 4 | 5 |
| | 2 | Investigating Cloud Services | Level 2 - Beginner | 2 | 4 | 5 |
| | 3 | Investigating Denial-of-Service Attacks | Level 4 - Proficient | 4 | 4 | 5 |
| | 4 | Dynamic Malware Analysis | Level 3 - Competent | 3 | 4 | 5 |
| | 5 | Static Malware Analysis | Level 4 - Proficient | 4 | 4 | 5 |
| | 6 | Network Forensics and Investigations | Level 3 - Competent | 3 | 4 | 5 |
| | 7 | Live System Forensics | Level 2 - Beginner | 2 | 4 | 5 |
| | 8 | Wireless and Network Hacking | Level 4 - Proficient | 4 | 4 | 5 |
| | 9 | Online Payments and Banking Fraud | Level 2 - Beginner | 2 | 4 | 5 |
| | 10 | Botnets & Underground markets | Level 3 - Competent | 3 | 4 | 5 |

Figure 22 is the resulting competency assessment skills matrix for Cyber Security Investigations - created by the DF-C$^2$M$^2$ assessment tool, illustrating actual skills rating (Red) versus required (blue) and the maximum possible rating (5) in purple:

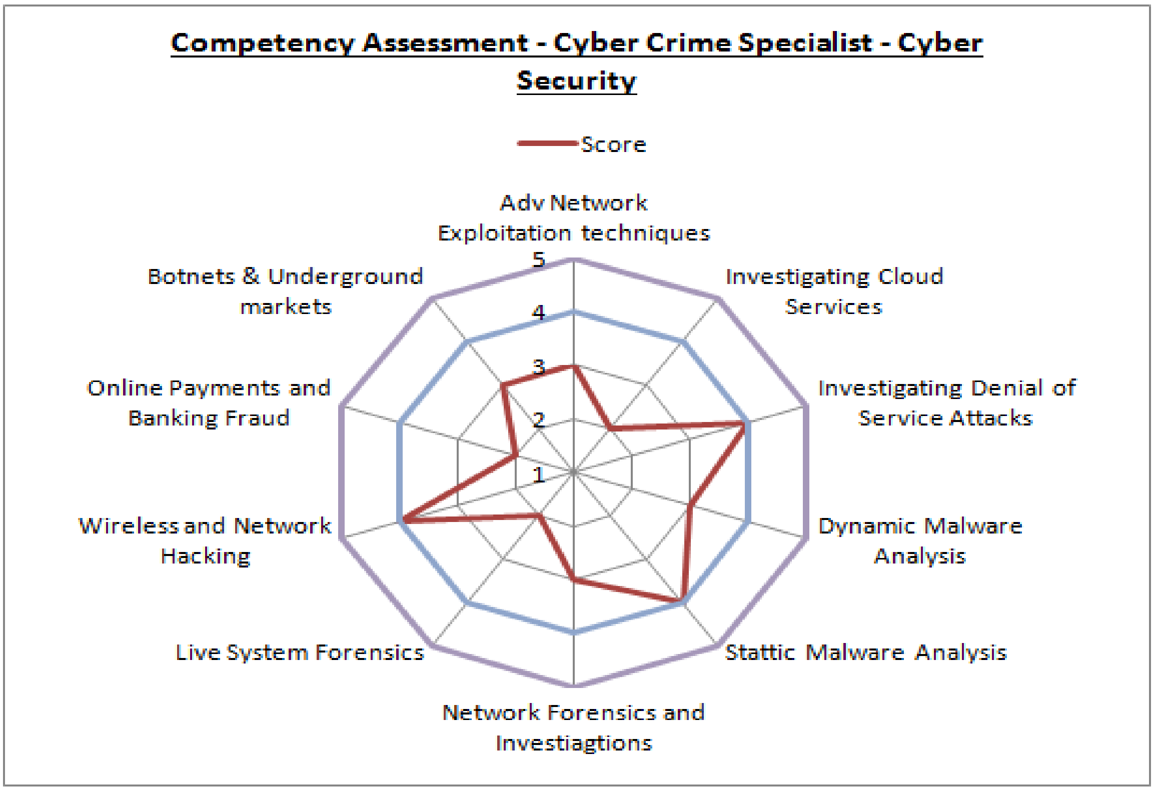


Figure 22: DF-C$^2$M$^2$ sample cybercrime investigation specialist ratings

Within the DF-C$^2$M$^2$, the above sample areas of assessment criteria were drawn from the DF-C$^2$M$^2$ Training and Career progression plan for cybercrime technical personnel as shown in Figure 23.

The DF-C$^2$M$^2$ suggested Cybercrime investigator skills progression and ratings have been included as a demonstration of the benefit of using the DF-C$^2$M$^2$ modular framework to expand and extend its application, as part of the future-proof, modular, and flexible design goal stated in Chapter 1.

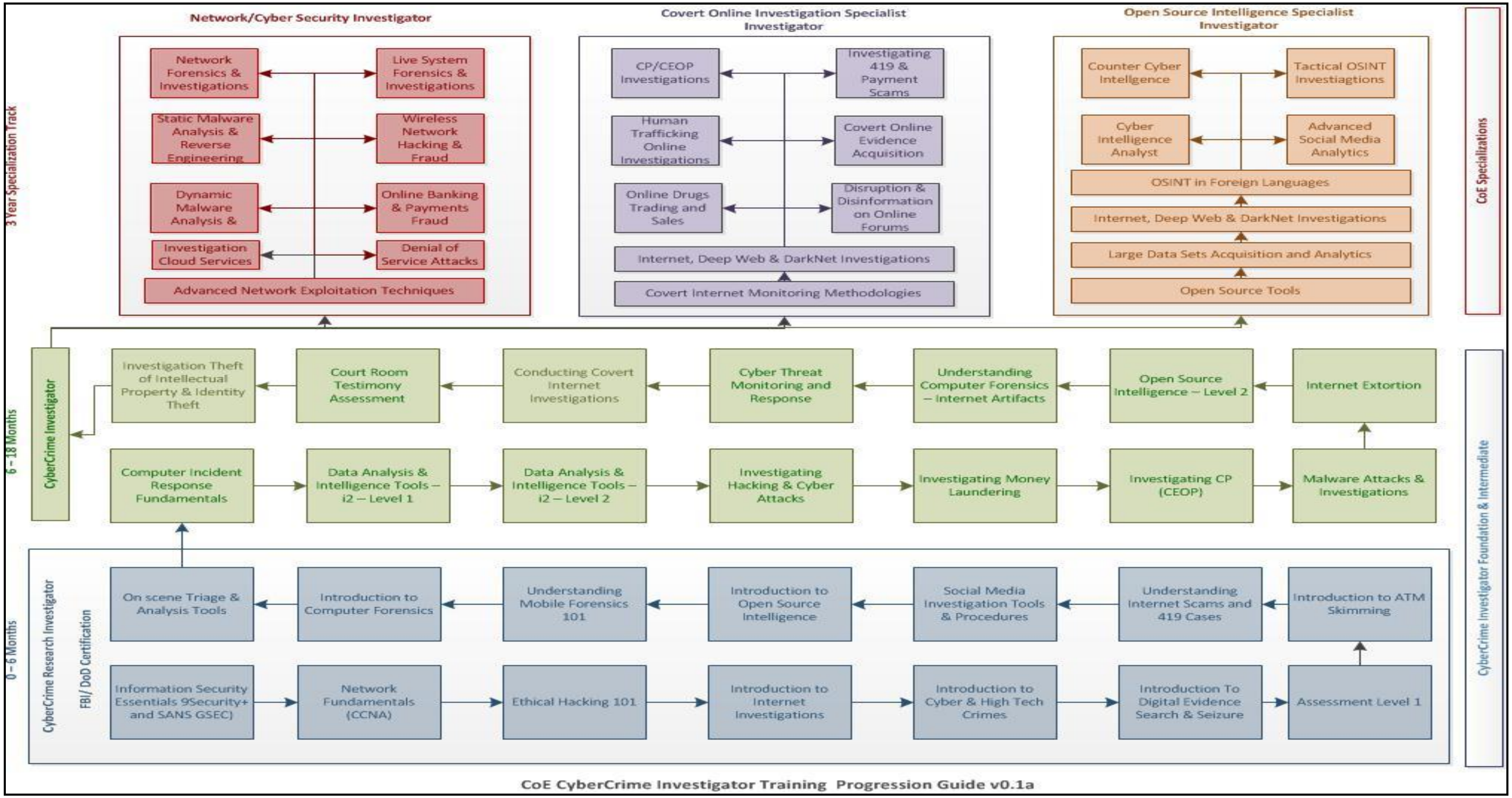

Network/Cyber Security Investigator
Network Forensics & Investigations
Live System Forensics & Investigations
Static Malware Analysis & Reverse Engineering
Wireless Network Hacking & Fraud
Dynamic Malware Analysis &
Online Banking & Payments Fraud
Investigation Cloud Services
Denial of Service Attacks
Advanced Network Exploitation Techniques
Covert Online Investigation Specialist Investigator
CP/CEOP Investigations
Investigating 419 & Payment Scams
Human Trafficking Online Investigations
Covert Online Evidence Acquisition
Online Drugs Trading and Sales
Disruption & Disinformation on Online Forums
Internet, Deep Web & DarkNet Investigations
Covert Internet Monitoring Methodologies
Open Source Intelligence Specialist Investigator
Counter Cyber Intellgence
Tactical OSINT Investiagtions
Cyber Intelligence Analyst
Advanced Social Media Analytics
OSINT in Foreign Languages
Internet, Deep Web & DarkNet Investigations
Large Data Sets Acquisition and Analytics
Open Source Tools
3 Year Specialization Track
CoE Specializations
6 – 18 Months
CyberCrime Investigator
Investigation Theft of Intellectual Property & Identity Theft
Court Room Testimony Assessment
Conducting Covert Internet Investigations
Cyber Threat Monitoring and Response
Understanding Computer Forensics – Internet Artifacts
Open Source Intelligence – Level 2
Internet Extortion
Computer Incident Response Fundamentals
Data Analysis & Intelligence Tools – i2 – Level 1
Data Analysis & Intelligence Tools – i2 – Level 2
Investigating Hacking & Cyber Attacks
Investigating Money Laundering
Investigating CP (CEOP)
Malware Attacks & Investigations
0 – 6 Months
CyberCrime Research Investigator
FBI/ DoD Certification
On scene Triage & Analysis Tools
Introduction to Computer Forensics
Understanding Mobile Forensics 101
Introduction to Open Source Intelligence
Social Media Investigation Tools & Procedures
Understanding Internet Scams and 419 Cases
Introduction to ATM Skimming
Information Security Essentials 9Security+ and SANS GSEC)
Network Fundamentals (CCNA)
Ethical Hacking 101
Introduction to Internet Investigations
Introduction to Cyber & High Tech Crimes
Introduction To Digital Evidence Search & Seizure
Assessment Level 1
CyberCrime Investigator Foundation & Intermediate
CoE CyberCrime Investigator Training Progression Guide v0.1a

**Figure 23: DF-C²M² cybercrime investigator career progression and training Guide**

]

### 6.5.3 Assessing Competency of Cybercrime & Digital Forensic Evidence Judiciary

It was acknowledged by workshop participants during the research that the knowledge of members of the Judiciary related to the concepts of Digital Evidence and Cybercrime could potentially affect the admissibility of certain evidence and the outcome of cases, and therefore should be considered as essential for any national bodies or law enforcement entities implementing the DF-C$^2$M$^2$.

Although not directly related to digital forensic organisational maturity, this concern was cited by several of the more experienced and senior practitioners interviewed and, in their view, affected the level of additional work required to assist in briefing prosecutors (and sometimes investigators) on the significance or meaning of evidential artefacts found during digital forensic examinations. It was therefore included as an option to demonstrate the modularity of the DF-C$^2$M$^2$ Framework.

These more experienced and senior practitioners felt that Organisational Maturity cannot be fully realised without finding a way to address this issue, thus helping free digital forensic personnel resources from having to undertake mundane ‘educational’ tasks.

Based on that and again as a demonstration of the DF-C$^2$M$^2$’s modular design goals, the need for Competency assessments of non-technical legal personnel were included within the scope of the DF-C$^2$M$^2$ as an option, and related foundational digital forensic concepts training material was created as part of the DF-C$^2$M$^2$ Body of Knowledge.

A set of requirements was created based on interviews conducted and feedback from the more experienced Digital Forensic Examiners who regularly work with members of the Judiciary (specifically prosecutors). These requirements for each role were identified during the investigation stage of this research and used to create a recommended training and competency testing plan for members of the judiciary.

The DF-C$^2$M$^2$ also prescribes a proposed training for members of the Judiciary that was cited as a limitation during earlier surveys and interviews, and therefore includes part of the Body of Knowledge as a means to help address issues related to understanding of digital forensics terms and principles for non-technical personnel.

## 6.6. DF-C²M² PROCESS DOMAIN - ASSESSMENT TOOL

According to the lab managers involved in the evaluation of the model; the most significant part of the DF-C²M² Model, Body of Knowledge, and Assessment tool is dedicated to process-related items and the Process domain. The Process domain of the DF-C²M² and Assessment covers four specific areas, namely:

1. Policies and Procedures
2. Best Practices
3. Standards (National and International)
4. Provision for Regulatory and Legal Requirements.

The DF-C²M² Best Practices assessment requirements include:

- General Best Practices
- Technical Best Practices
- Quality Management Best Practices
- The DF-C²M² Policies Assessment and Audit Criteria

### 6.6.1 Assessment Criteria for Use and Conformance with Best Practices

Best practices were often cited as critical in the absence of a defined standard for a particular subject. Conformance with best practices as stated in Chapters 1 and 5 were therefore equally important to ISO 17025.

Thus, provision of measuring conformance with a list of established and accepted ‘de facto’ best practices were established and factored into the DF-C²M² Model, Assessment Tool, and Body of Knowledge.

Tables 24, 25, and 26 represent sample criteria used to check and assess various types of compliance with a variety of industry-accepted best practices drawn from NIST, SWGDE, NIJ and APCO. The list of best practices referenced in provided in Appendix J.

## 1. Conformance with Best Practices in General:

Table 24: Conformance with general best practices

| Category | Description | Score | | |
|---|---|---|---|---|
| | | Level | Rating | Required |
| **GPB** | **General Best Practices** | | | |
| GPB1 | Lab policies encourage and promote the development, use, and sharing of best practices. | Level 4 - Measured & Automated | **4** | **5** |
| GPB2 | Lab uses industry-accepted best practices/standards for all technical and evidence handling aspects. | Level 4 - Measured & Automated | **4** | **5** |
| GPB3 | Lab methods for tools and process are based on a reference industry's accepted best practices. | Level 2 - Partial Deployment | **2** | **5** |
| GPB4 | Lab publishes selected internal best practices for peer review at least twice per annum. | Level 4 - Measured & Automated | **4** | **5** |
| GPB5 | External best practices references are revised and updated as may be required and are referenced. | Level 4 - Measured & Automated | **4** | **5** |
| GPB6 | Best practices used for Imaging. | Level 4 - Measured & Automated | **4** | **5** |
| GPB7 | Best Practices used for Computer Examination with Encase. | Level 4 - Measured & Automated | **4** | **5** |
| GPB8 | Best Practices used for Computer Examination with FTK. | Level 4 - Measured & Automated | **4** | **5** |
| GPB9 | Best Practices used for Computer Examination with Xways. | Level 4 - Measured & Automated | **4** | **5** |
| GPB10 | Best Practices used for Mobile Examination with XRY. | Level 4 - Measured & Automated | **4** | **5** |

## 2. Conformance and Use with Technical Best Practices:

Table 25: Conformance with technical speciality areas best practices

| Category | Description | Score | | |
|---|---|---|---|---|
| | | Level | Rating | Required |
| TBP | Technical Best Practices | | | |
| TBP1 | ACPO Principles | Level 3 - Full Deployment | 3 | 5 |
| TBP2 | SWGDE Imaging | Level 4 - Measured & Automated | 4 | 5 |
| TBP3 | SWGDE Mobiles | Level 4 - Measured & Automated | 4 | 5 |
| TBP4 | Internal Media Wiping | Level 4 - Measured & Automated | 4 | 5 |
| TBP5 | Encase (Developed in-house) | Level 5 - Continuously Improving | 5 | 5 |
| TBP6 | Password Recovery (Developed in-house) | Level 5 - Continuously Improving | 5 | 5 |
| TBP7 | Live Memory/RAM Analysis | Level 4 - Measured & Automated | 4 | 5 |
| TBP8 | Workstation Verification (based on DFRWS) | Level 4 - Measured & Automated | 4 | 5 |
| TBP9 | Media Wiping and Verification | Level 3 - Full Deployment | 3 | 5 |

## 3. Conformance with Legal and Regulatory Requirements (Generic):

Sample extracts for each of these taken from the DF-C²M² Assessment tool is for Legal and Regulatory areas shown below:

Table 26: Conformance with local legal and regulatory requirements

| Category | Description | Score | | |
|---|---|---|---|---|
| | | Level | Rating | Required |
| | Conformance with Legal Requirements (Country-specific) | | | |
| L1 | The request includes duly authorised warrant or equivalent. | Level 4 - Measured & Automated | 4 | 5 |
| L2 | Examiner opinions not expressed in the report. | Level 4 - Measured & Automated | 4 | 5 |
| L3 | The report presents data in non-technical terms. | Level 2 - Partial Deployment | 2 | 5 |
| L4 | The report is duly signed, stamped, and admissible in court. | Level 4 - Measured & Automated | 4 | 5 |
| L5 | Request reviewed with the Investigator / Prosecutor. | Level 4 - Measured & Automated | 4 | 5 |
| L6 | Results reviewed with the Investigator / Prosecutor. | Level 4 - Measured & Automated | 4 | 5 |

## 6.7 DF-C$^2$M$^2$ TOOLS - ASSESSMENT TOOL

Validation and testing of Tools and methods was cited by survey and workshop participants as a major time-consuming challenge that labs routinely faced as stated in Chapter 1. The result was that some labs opted to use older, outdated tools rather than to test newer versions and therefore risk missing evidential items, as discussed in Chapter 5.

The Tools domain of the DF-C$^2$M$^2$ Model Assessment covers two specific areas, namely related to Tools:

1. Validation of Tools
2. Validation of Methods

Sample DF-C$^2$M$^2$ assessment requirements for each of these areas are covered in Table 27 through Table 29:

1. **Validation of Tools Sample Assessment Criteria (includes People- and Process-related requirements):**

   The sample extract below shows the integration of both People and Process requirements within the Tool validation assessment criteria as described as essential in Chapter 5 – Service Catalogue Impact vs. Complexity.

Table 27: Compliance criteria for validation of tools

| Category | Description | Score | | |
|---|---|---|---|---|
| | | Level | Rating | Required |
| **VT** | **Validation of Tools** | | | |
| VT1 | All Primary Tools used are validated. | Level 4 - Measured & Automated | 4 | 5 |
| VT2 | The lab has procedures to test and validate tools. | Level 4 - Measured & Automated | 4 | 5 |
| VT3 | Lab uses external validation results from established bodies such as NIST, etc. | Level 2 - Partial Deployment | 2 | 5 |
| VT4 | The lab has test data sets for tools testing. | Level 4 - Measured & Automated | 4 | 5 |
| VT5 | The lab has a well-documented testing and validation process. | Level 4 - Measured & Automated | 4 | 5 |
| VT6 | Qualified Personnel conduct testing of tools. | Level 4 - Measured & Automated | 4 | 5 |
| VT7 | Validation test results are documented with data sets and retained indefinitely. | Level 4 - Measured & Automated | 4 | 5 |
| VT8 | Validation test results are shared with the vendor (where issues arise). | Level 4 - Measured & Automated | 4 | 5 |
| VT9 | Validation test results are shared with other legally authorised peer labs. | Level 4 - Measured & Automated | 4 | 5 |
| VT10 | Personnel are trained on any new tools prior to implementation/authorisation. | Level 4 - Measured & Automated | 4 | 5 |
| VT11 | Personnel are competency tested on new tools prior to implementation. | Level 4 - Measured & Automated | 4 | 5 |
| VT12 | Workstation baseline builds are systematically updated with new tools. | Level 4 - Measured & Automated | 4 | 5 |
| VT13 | Technical SOPs and references are updated prior to implementation of new tools. | Level 4 - Measured & Automated | 4 | 5 |
| VT14 | Updates to tools are first reviewed and approved prior to implementation. | Level 4 - Measured & Automated | 4 | 5 |
| VT15 | All validation tests are technically reviewed to ensure results are repeatable. | Level 4 - Measured & Automated | 4 | 5 |
| VT16 | Provision with QMS for deviation from using standard tools in exceptional cases. | Level 4 - Measured & Automated | 4 | 5 |

2. **Validation of Methods, Sample Assessment Criteria (includes People- and Process-related requirements):**

   As stated in Chapter 5, the validation of Tools within the Tools domain extends to the validation of methods, which is deemed to be equally important when looking at tool validation and testing. Validation of methods is often overlooked by lab personnel and is regarded as being non-essential, and many stated that they would not know how to validate a method. The sample criteria below should assist in addressing these various issues discovered during this research.

**Table 28: Compliance criteria for validation of methods**

| Category | Description | Score | | |
|---|---|---|---|---|
| | | Level | Rating | Required |
| **VM** | **Validation of Methods** | | | |
| VM1 | All Technical Methods used are validated to ensure evidential integrity. | Level 4 - Measured & Automated | **4** | **5** |
| VM2 | The lab has procedures to test and validate new methods. | Level 4 - Measured & Automated | **4** | **5** |
| VM3 | Lab uses external validation results from established bodies such as NIST, etc. | Level 2 - Partial Deployment | **2** | **5** |
| VM4 | The lab has test data sets for new testing methods. | Level 4 - Measured & Automated | **4** | **5** |
| VM5 | The lab has a well-documented testing and validation process. | Level 4 - Measured & Automated | **4** | **5** |
| VM6 | Qualified Personnel conduct design and testing of new methods. | Level 4 - Measured & Automated | **4** | **5** |
| VM7 | Validation test results are documented with data sets and retained indefinitely. | Level 4 - Measured & Automated | **4** | **5** |
| VM8 | Validation test results are shared with other legally authorised peer labs. | Level 4 - Measured & Automated | **4** | **5** |
| VM9 | Personnel are trained on any new methods prior to implementation/authorisation. | Level 4 - Measured & Automated | **4** | **5** |
| VM10 | Personnel are competency tested on new methods prior to implementation. | Level 4 - Measured & Automated | **4** | **5** |
| VM11 | Technical SOPs and references are updated prior to implementation of new methods. | Level 4 - Measured & Automated | **4** | **5** |
| VM12 | Updates to methods are first reviewed and approved prior to implementation. | Level 4 - Measured & Automated | **4** | **5** |
| VM13 | All validation tests are technically reviewed to ensure results are repeatable and based on Best Practices/Standards. | Level 4 - Measured & Automated | **4** | **5** |

3. **Validation of Tool – General Ratings**

The following provides a general summary of some of the criteria used to assess the organisation's posture regarding use and validation of tools:

Table 29: Validation of tools - general ratings

| Category | Description | Score | | |
|---|---|---|---|---|
| | | Level | Rating | Required |
| **To** | **Tools** | | | |
| To1 | Only tools that have been validated are used for digital evidence acquisition, examination, and analysis. | Level 3 - Full Deployment | **3** | **5** |
| To2 | All primary forensic hardware and software is verified to determine if it functions as expected prior to the start of each new case/examination. | Level 2 - Partial Deployment | **2** | **5** |
| To3 | Potential issues or errors with any tools used are documented and submitted to the supplier for resolution, and subject to the impact of the evidence/findings may require the use of a tool to be suspended until the issue is resolved. | Level 2 - Partial Deployment | **2** | **5** |

## 6.8 SUMMARY

This chapter has highlighted the key elements of the DF-C$^2$M$^2$. The DF-C$^2$M$^2$ Assessment tool has dual purposes in that it lists the DF-C$^2$M$^2$ requirements for each of the three core domains, and provides a way to measure compliance with these requirements.

The DF-C$^2$M$^2$ Body of Knowledge presents the key components of the final deliverable of this research. Presently, only sample extracts of the Body of Knowledge have been highlighted in this chapter. At present, the DF-C$^2$M$^2$ Knowledge Base exists as a series of documents, workflows, and spreadsheets categorised based on key Domain (People, Processes, and Tools), available for review and issued as a standalone document titled DF-C$^2$M$^2$ Body of Knowledge version 1.1. (See the Footnote)[6]

Work on the DF-C$^2$M$^2$ Body of Knowledge and on packaging the model and its deliverables in a simple-to-use and -follow system are still in progress, although the model is implementable and available as a complete deliverable at present.

In summary, the design and implementation of the DF-C$^2$M$^2$ Model and the creation of the DF-C$^2$M$^2$ Assessment Tool resulted in a usable DF-C$^2$M$^2$ Body of Knowledge that provides:

1. A considerable body of work and accumulated heuristic knowledge that can be applied to augment current systems and processes within a digital forensic lab.
2. Provide a method to incorporate Capability Maturity into various processes as they relate to People, Processes, and Tools.
3. A readily extensible repository of information that can be updated and additional requirements added in the future, enabling it to be adapted to incorporate future ISO digital forensics-related standards.
4. A common set of criteria that can be used for Digital Forensic Lab ISO 17025 and Capability Maturity Assessment and Readiness evaluations.
5. A platform to enable future inter-lab and practitioner collaboration towards developing digital forensics best practices and specific standards.

[6] https://www.dropbox.com/sh/nguilxkgfaryyfx/AACS6r5I-qSrSka4OlGSIvsoa?dl=0

6. A repository of digital forensic lab-specific standardised workflows and standard operating procedures (SOPs) related to Digital Forensics tasks and processes.

The key design goals for the DF-C$^2$M$^2$ were validated, and based on participating practitioners' feedback the design goals were achieved, but would need to be fully tested on a larger scale with more participating laboratories in future. The model's effectiveness as a performance planning and improvement tool is detailed in the sample lab assessments using the DF-C$^2$M$^2$ in Chapter 7. Feedback on the model, the various tools, and Body of Knowledge are reviewed in more detail in Chapter 8.

Additionally, despite new ISO standards, specifically ISO 27041 and ISO 27042 being released in June 2015, the DF-C$^2$M$^2$ framework and Body of Knowledge already have catered to the requirements defined within these standards ahead of the standards' release and as validation of the design goals and holistic approach of DF-C$^2$M$^2$. ISO 27041 and ISO 27042 were not available as standards for reviews at the time of the participant reviews, and provision to add ISO 27041 and ISO 27042 specific references to enable easier cross-checking will later be implemented in the DF-C$^2$M$^2$ Assessment Tool later.

# CHAPTER 7: DF-C$^2$M$^2$ - APPLIED ASSESSMENT AND EVALUATION RESULTS

## 7.0 INTRODUCTION

This chapter will provide details on the Digital Forensics – Comprehensive Capability Maturity Model (DF-C$^2$M$^2$) assessment of an existing ISO 17025 accredited laboratory, and a non-accredited digital forensic laboratory. This chapter will present the assessment findings and validation of the need for such a model such as the DF-C$^2$M$^2$ based on the assessment results and participant feedback. Participants' perceived strengths and limitations of the model will also be discussed, as will how they impact the model's present and future value proposition.

## 7.1 BACKGROUND

As part of the ongoing research into the need for a universally acceptable digital forensics-focussed framework for assessing, planning, and implementing digital forensic laboratories, a DF-C$^2$M$^2$ readiness assessment was conducted of an ISO 17025 accredited digital forensic laboratory, as well as of a newly established non-accredited digital forensic laboratory. These assessments helped to determine:

1. Applicability and relevance of the proposed DF-C$^2$M$^2$.
2. Practicality of the proposed DF-C$^2$M$^2$ assessment tools and methods.
3. DF-C$^2$M$^2$ as a digital forensics readiness tool.
4. Feedback on the DF-C$^2$M$^2$ benefits from practitioners within the labs.
5. Gaps and areas for improvement within DF-C$^2$M$^2$.
6. Feedback and recommendations on the DF-C$^2$M$^2$ (from participants).
7. Future areas of improvement and expanding the present Body of Knowledge.

The methods used for the DF-C$^2$M$^2$ readiness assessment were as defined within the proposed DF-C$^2$M$^2$ Introduction document – via accepted ISO audit practices, i.e. through a series of interviews, document reviews, and witnessing of tests, using the DF-C$^2$M$^2$ Assessment tool and supporting Body of Knowledge.

## 7.2 CONDUCTING AN ASSESSMENT USING DF-C$^2$M$^2$

### ASSESSMENT PROCESS

The DF-C$^2$M$^2$ assessment of participating labs was conducted more as a ‘consultative audit’ using the DF-C$^2$M$^2$ Assessment tool, and the assessment process involved:

1. Introductory meeting and overview with key stakeholders.
2. Reviewing processes and documentation.
3. Interviews with key administrative and a subset of select technical personnel.
4. Witnessing tasks and procedures.
5. Review of customer feedback.
6. Review of any relevant supporting documentation and records.
7. Soliciting feedback on the DF-C$^2$M$^2$ from participants.
8. Wrap-up summary meeting (Lab SWOT analysis based on the DF-C$^2$M$^2$).
9. Preparation of final report.
10. Presentation of final report to the assessed organisation.
11. Benchmarking the findings for future analysis and comparisons.

Initial assessed labs will have no benchmark data to be compared against, and as such, initial required scores are assuming Best Case scenarios. In the future, as more labs are assessed, benchmarking data will be maintained to compare labs in a similar category against each other to determine an industry/sector baseline. In all cases, the average minimum required DF-C$^2$M$^2$ per category evaluated should not be below an initial suggested minimum rating of **3.5** which was chosen as an initial baseline.

The rationale behind this minimum rating was that a rating of 3 would indicate Full Deployment within the DF-C$^2$M$^2$ assessment tool, and that labs should at least exceed this rating to demonstrate an acceptable degree of capability maturity in each of the three key domains. Participating practitioners mostly thought this was fair, however it was agreed by consensus that further assessments for other labs and feedback from a wider group of participants would be required in future to determine what the actual initial minimum rating should be, and over time with more participating labs, this minimum rating could be determined based on inter-lab comparison of results. Figure 17 illustrates the DF-C$^2$M$^2$ assessment tool structure.

The initial assessments of a relatively new ISO 17025 accredited lab will help to determine:

a) What a typical ISO 17025 accredited lab's ratings are for each category and help highlight areas not covered by ISO 17025, where such labs may be found to be lacking, but are considered to be essential to the lab's long-term effectiveness, efficiency, and quality of technical and procedural operations as defined within the DF-C²M².
b) Areas for improvement within the overall lab's current and future plans.
c) Practicality and utility of the DF-C²M² assessment process.
d) Areas for improvement within the DF-C²M² and the DF-C²M² assessment process.

### 7.2.1 Guidelines for the DF-C²M² Readiness Assessment

For each of the DF-C²M² requirements (assessment criteria), the assessor needed to consider:

1. Is the process/task currently being performed correctly?
2. Is the process/task adequately documented?
3. Is the task subject to ISO 17025/ASCLD-LAB, Daubert/Frye requirements?
4. Is the process/task well understood by those responsible for ensuring compliance and those performing the task?
5. Is the process/task auditable/verifiable? Can it be demonstrated and witnessed?
6. Under what circumstances have deviations from the documented process occurred? How were these documented and authorised? What corrective actions were taken to reduce the likelihood of repeated deviations?
7. Does the process cover all the essential steps based on industry best practices or standards, as well as additional steps to ensure optimum utilisation of resources?
8. Does the process lend itself to measurement and benchmarking (e.g. time taken to complete the process, or accuracy/completeness of the result)?
9. Can the personnel performing the task be rated using P-CMM?
10. For a given process, how is the process currently rated using CMM?
11. For a given process, can the tool(s) employed be rated using CMM?
12. Are any identified limitations on efficiency or accuracy of the process due to issues with Tools or Personnel (P-CMM)?
13. Does the DF-C²M² Assessment tool (and Body of Knowledge) address all tasks and their pre-requisites effectively?
14. How can the process or DF-C²M² element be improved?

## 7.3 UNDERSTANDING THE DF-C$^2$M$^2$ ASSESSMENT PROCESS KEY ELEMENTS

The key elements of the DF-C$^2$M$^2$ assessment that were performed during these assessments included:

### 7.3.1 Review Organisation's Service Offerings vs. the DF-C$^2$M$^2$ Service Catalogue

These assessments included reviewing the scope/comprehensiveness of the present service offerings (planned and current), the implementation status of each service, the impact vs. complexity ratings for each service, and whether a specific service was categorised as a Core, i.e. an essential/pre-requisite service, or Value-Added, i.e. an optional, service.  Core vs Value-Added service categories were defined by an analysis of which services are commonly provided by the digital forensic labs, and considered to be essential, versus which services would be nice to have, but non-essential for the majority of all the examination tasks carried out by the labs assessed. The consensus opinion amongst evaluation participants specifically the lab managers/lab manager designees was that those services designated as 'Core' were mostly essential, but opinions differed as to whether Value Add should be defined within the service catalogue if they are deemed non-forensic evidence specific.

Lastly, a review was conducted of whether or not a defined Service Catalogue existed, if the services made available were communicated with the digital forensic lab's customers, and if the catalogue clearly defined:

- The nature/description of the service.
- Any known limitations of the service.
- Any defined/expected service levels for the service, and
- Availability of the service.

#### 7.3.1.1 The Role of the DF-C$^2$M$^2$ Service Catalogue

Within the DF-C$^2$M$^2$, a published Service Catalogue is considered a key planning tool, and a key customer tool for understanding what services are available, the applicability of each service, levels of authorisations that may be required, and planned Service Level Targets for each service.

The identification of dependent services within the Service Catalogue is also considered vital to helping lab management to ensure that all prerequisite requirements for the successful delivery and implementation of a service have been clearly identified, planned for, and included within the digital forensic laboratory's Quality Management System, and related policies and procedures governing People, Processes, and Tools.

Additionally, the Service Catalogue provides a means to assess if all required/essential services have been identified. Later on and during the assessments, the Service Catalogue also serves as a tool to determine if the relevant skills, tools, and processes for each defined service are available, and if they have been reviewed and assessed for their suitability to meet the current requirements of the service.

The lack of a documented service catalogue would be considered as a major shortcoming within the planning and development stages of a digital forensic laboratory, and a provisional Service Catalogue would be used as stopgap measure to assist with the assessment. This step would require that an initial assessment be conducted to determine the services and service levels for each lab.

The prerequisites for each service presently defined within the DF-C$^2$M$^2$ Service Catalogue are well-defined, and therefore these prerequisites could also be used as part of the audit to determine any non-conformances or oversights that may indicate that the audited lab does not meet the DF-C$^2$M$^2$ required prerequisites for the delivery of a given service. A documented Service Catalogue within the DF-C$^2$M$^2$ may be considered as the high-level blueprint for a digital forensic laboratory that helps a laboratory to clearly define:

a. What services do they need to versus wish to provide?
b. What are the requirements to successfully implement and deliver this service (People, Processes, and Tools)?
c. What are the associated service dependencies and prerequisites for the delivery of each service?
d. What services are considered to be essential (Core) and therefore should have a higher priority (budget, training, etc.), versus what services would be rather 'nice to have' or be considered value-added services?
e. What are the known limitations or prerequisites for each service that the customer should be aware of?
f. Which services should be implemented first, and which services can be implemented at a later stage?

g. What Service Level Targets apply to each service? (Based on the lab's current state (People, Processes, and Tools).)
h. How do we categorise services (and any related specialisations)?

Additionally, each service listed within the Service Catalogue should be reviewed at least annually to determine:

1. Relevance to current and future business operations.
2. Impact vs. Complexity.
3. The options of in-sourcing vs. out-sourcing to qualified contractors based on cost, confidentiality, and required service levels.
4. Number of services requests received where this service was required and utilised or not available.
5. Envisioned future requests for such services, e.g. technology/device is soon to be obsolete.

The DF-C²M² Service Catalogue is designed to cover a broad range of commonly requested digital forensic lab services drawn from the specialised fields of Computer Forensics, Mobile Forensics, Digital Video Forensics, Network Forensics, and Technical Investigations Support Services. The six main categories of services covered by the DF-C²M² Service Catalogue are as follows:

1. Computer Forensics (CF).
2. Mobile Handset Forensics (MHF).
3. Digital Audio and Video Forensics (DA&VF).
4. Network Forensics (NF).
5. Digital Evidence Tactical Support (DETS).
6. Cyber Crime Investigation Support (CIS).

**Note:** For each service within the above categories, the DF-C²M² provides a detailed service description that details:

- Service objective and definition.
- Service context and known dependencies or limitations.
- Tier of customers who can access the service (optional).

- Phase of the digital forensic lab development/roadmap when the service will be 'activated' or made available to customers.
- Functions and prerequisites associated with the delivery of service.
- How the priority level of each service is determined?

It was determined through the discussions and feedback from the participants during the workshop that the DF-C²M² Service Catalogue addresses the majority of all services that a lab may be requested to provide.

#### 7.3.1.2 Modularity of Assessment Process/Options

While being extensive in terms of the ranges of the service categories covered by the DF-C²M² Service Catalogue, it is still modular by design, and therefore offers flexibility – enabling organisations to implement service categories that only relate to their specific types of examinations offered; for example, a telecommunications company may implement only those service categories related to the types of investigations they are authorised to or need to examine, e.g.: Computer Forensics (CF), Network Forensics (NF), and possibly Mobile Handset Forensics (MHF), etc. In such a case, the organisation would need to address the DF-C²M² People, Processes, and Tools requirements for the delivery of each of the three aforementioned service categories.

Additionally, within the DF-C²M², the laboratory's Scope of accreditation as defined under ISO 17025/ASCLD-LAB requirements would specifically identify the areas the laboratory is accredited for. Typically, the three areas of accreditation under ISO 17025 and ASCLD/LAB map to the DF-C²M², Computer Forensics, Digital Video Forensics, and Mobile Phone Forensics 'Core Services'.

### 7.3.2 Addressing Organisational Differences in the DF-C²M² for (Law Enforcement, Non-Law Enforcement)

The DF-C²M² Assessment covers the People, Processes, and Tools readiness requirements for each of the steps in the DF-C²M² Six Steps Model, namely Assessment, Collection, Examination, Analysis, Reporting, and Review.

The DF-C²M² model enables organisational differences to be factored into policies and procedures governing People, Processes, and Tools. For example, requirements for Law Enforcement (i.e. criminal investigation digital forensic laboratories) and non-Law Enforcement (e.g. commercial entities) have certain key elements considered as mandatory within the DF-C²M², and yet also have provisions for other elements that may be regarded as optional depending on the nature of the organisation and the typical types of cases it handles, e.g. levels of authorisation required to conduct a human resource violation investigation, versus a criminal financial fraud investigation.

#### 7.3.2.1 The DF-C²M² People Requirements

The People requirements assessment looks at job descriptions, authority to perform duties, role-specific training and career development plans, conformance with training requirements, competency testing for each key role, proficiency testing, and People Capability Maturity (P-CMM).

**Note:** In general, the People, Tools, and Processes requirements for both Law Enforcement and Non-LE digital forensic laboratories are the same within the DF-C²M², but provision is made to accommodate any differences or additional requirements that may be required, for example, levels of security clearance based on case type within a Law Enforcement laboratory.

#### 7.3.2.2 The DF-C²M² Process Requirements

The Process requirements assessment covers several areas related to having structured formalised and reviewed processes for areas related to Quality Management, Operations, Health, Safety, Training, Technical Processes, and process Capability Maturity (CMM).

Each area is assessed to determine if the processes exist, whether they are adequately documented, whether the processes are effective, if there is proof of implementation, and if there is an audit and corrective process to detect and resolve any issues.

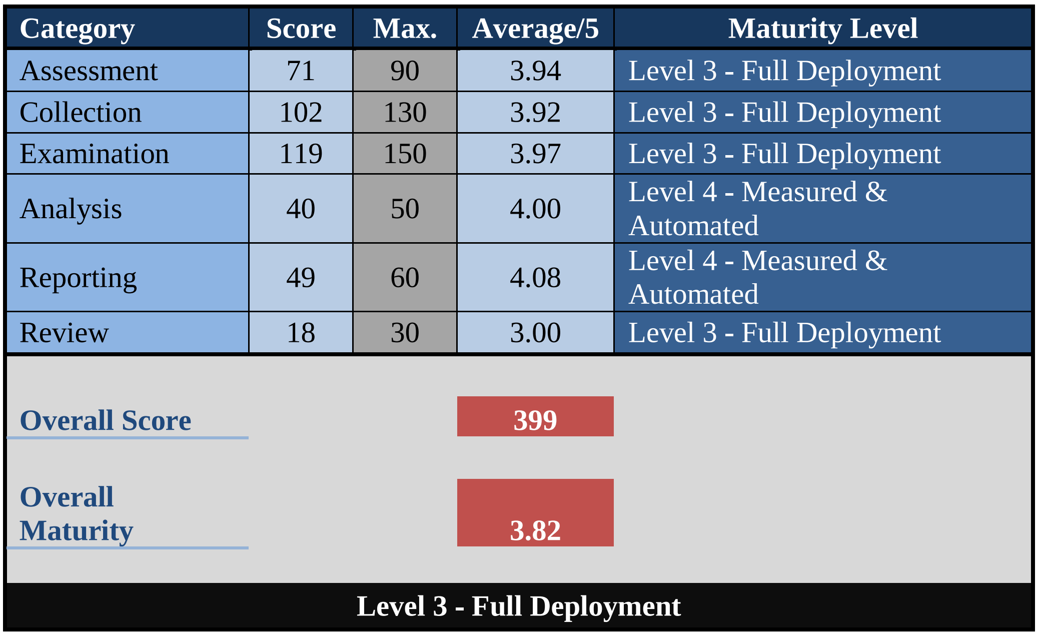
#### 7.3.2.3 The DF-C²M² Tools Requirements

The assessment helps determine the accuracy and thoroughness of tool and method testing and approvals, authorisations to use specific tools (based on training and competence), and the effectiveness of the tool and method testing system in use (Tools Capability Maturity).

### 7.3.3 DF-C$^2$M$^2$ Reporting and Assessment Results

Upon completion of the assessment, a DF-C$^2$M$^2$ compliance report is produced that is reviewed with the assessed organisation and discussed in order to help them determine a roadmap to address any non-compliances, and as a means to provide a roadmap to help improve the overall quality and efficiency of the organisation's digital forensic laboratory and service offerings. Figure 24 to Figure 26 show samples from the readiness assessment results.

The results of the assessment would in the future be maintained within a database to help determine the baseline for a similar lab and to enable inter-lab benchmarking of compliance.



| Category | Score | Max. | Average/5 | Maturity Level |
|---|---|---|---|---|
| Assessment | 71 | 90 | 3.94 | Level 3 - Full Deployment |
| Collection | 102 | 130 | 3.92 | Level 3 - Full Deployment |
| Examination | 119 | 150 | 3.97 | Level 3 - Full Deployment |
| Analysis | 40 | 50 | 4.00 | Level 4 - Measured & Automated |
| Reporting | 49 | 60 | 4.08 | Level 4 - Measured & Automated |
| Review | 18 | 30 | 3.00 | Level 3 - Full Deployment |
| Overall Score | | | 399 | |
| Overall Maturity | | | 3.82 | |
| Level 3 - Full Deployment | | | | |

Figure 24: DF-C$^2$M$^2$ Tool: maturity level assessment

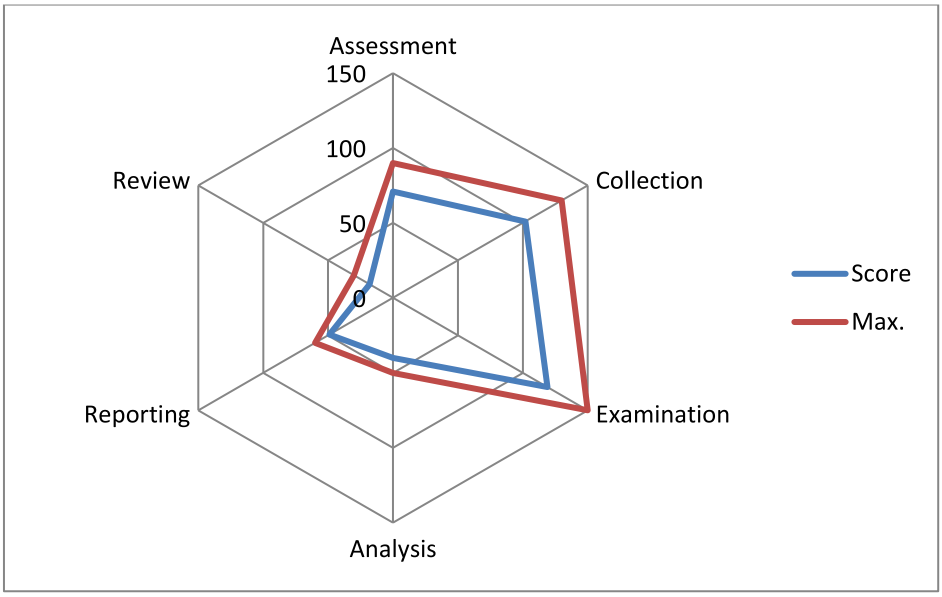


**Figure 25: DF-C$^2$M$^2$ Tool: readiness assessment results - current vs. required**

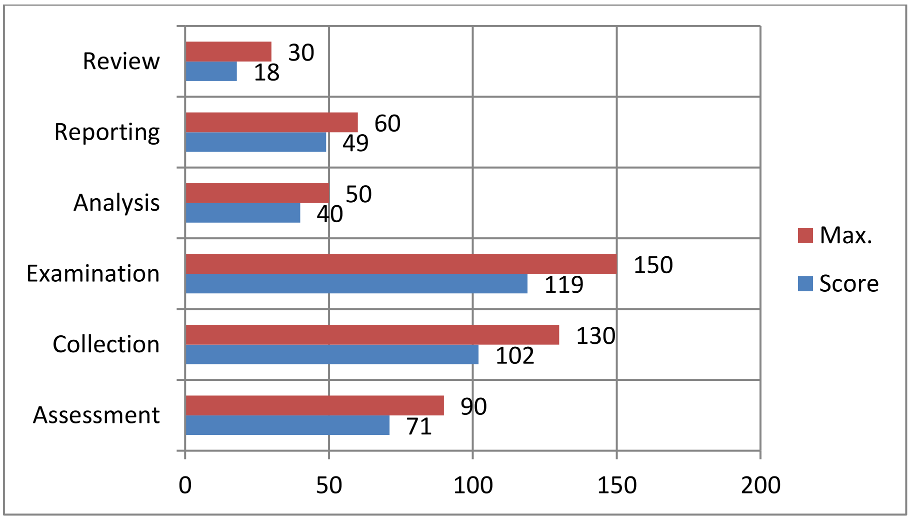


**Figure 26: DF-C$^2$M$^2$ Tool: readiness assessment – rating vs. industry benchmark**

## 7.4 DF-C$^2$M$^2$ ASSESSMENTS OF PARTICIPATING LABS

Of the two volunteer labs that participated in the DF-C$^2$M$^2$ assessment, one lab was a relatively well-established, ISO 17025 accredited digital forensic lab within the Law Enforcement sector, whilst the other was a newly established academic lab.

The lab assessment exercises performed were multi-purpose. By evaluating two labs with completely different core business focusses and requirements, the goal was to help determine:

1. The applicability of the DF-C$^2$M$^2$ to labs with different organisational and business requirements.
2. The flexibility and relevance or value of the DF-C$^2$M$^2$ to various types of digital forensic laboratories, at different stages of their development, and that offer a different range of services, with different capabilities and sizes.
3. Suitability of the DF-C$^2$M$^2$ Assessment Tool and underlying DF-C$^2$M$^2$ Service Catalogue to help facilitate more holistic and detailed laboratory audits and assessments.
4. Gain practitioner feedback and insight on issues and their perceived value of the DF-C$^2$M$^2$.
5. Assess any possible limitations of the DF-C$^2$M$^2$ and its approach that could be used to improve on it.
6. Observations and reflections on the DF-C$^2$M$^2$ framework components.

Details of both laboratories and the findings based on the DF-C$^2$M$^2$ assessments are discussed in this chapter.

### 7.4.1 Lab #1 Background

Lab #1 was an established lab that had been in operation for just over three years. The lab was ISO 17025 accredited and had experienced rapid growth and development within its first three years. The lab had ambitious goals and objectives in addition to finding ways to enhance its capability and range of services.

The facility had been designed to offer a range of services in support of criminal investigations, and was staffed by a rapidly growing team of experienced and qualified practitioners[7].

Maintaining ISO 17025 accreditation was a mandatory key goal for this lab; however, faced with a growing number of cases, increased volume of data to analyse [8], and having to rapidly employ and train additional staff, Lab #1 envisaged challenges further down the line that would require it to find ways to work smarter and more effectively.

Lab #1 provided a seasoned pool of practitioners and relatively mature processes to validate DF-C$^2$M$^2$ against. Lab #1 would provide much potential insight into any DF-C$^2$M$^2$ limitations and suitability for use within well-established digital forensic laboratories.  This data would also serve as part of the data for possible future benchmarking exercise with other comparable labs.

Lab #1 would prove to be an ideal and challenging environment to test the DF-C$^2$M$^2$ framework, Assessment tool, Body of Knowledge, and to ultimately test its value proposition.

[7] All examiners that participated held an MSc in Digital Forensics or Information Security, or were about to complete their MSc in Digital Forensics.

[8] Based on interview with Lab #1 senior personnel.

### 7.4.2 Lab #2 Background

A non-accredited, newly established laboratory within a higher education academic environment. The lab catered to students studying for the BSc and MSc in Information Security curricula, which included digital forensics. The lab facility was designed to support students and fictitious cases and scenarios. However, Lab #2 expressed that is was keen to assess the DF-C$^2$M$^2$ with the goal of being able to provide services to a broader range of customers, and in line with international standards and best practices for potentially both civil investigations and disputes.

Gaining ISO 17025 accreditation was not a major motivating factor for Lab #2 at the time of the assessment. The reasons cited for not pursuing ISO 17025 accreditation at this early stage of the laboratory's development was due to the perceived cost and complexity of preparing for, gaining, and the maintaining accreditation.

Lab #2 therefore proved to be an ideal testing ground to help assess the strength of the DF-C$^2$M$^2$'s People, Processes, and Tools value proposition.

### 7.4.3 DF-C²M² Lab Assessment and Feedback Process Outline

Several activities were performed as part of the assessments of each participating lab following the obtaining of written approvals and consent to use the findings as part of this research. The assessment plan and steps taken during each assessment are listed in Table 30.

Table 30: DF-C²M² review and assessment key milestones

| # | Assessment Activity Description/Summary | Completed Lab #1 | Completed Lab #2 | Completed Student Group |
|---|---|---|---|---|
| 1 | DF-C²M² introductory presentation, goals | Y | Y | Y |
| 2 | DF-C²M² Body of Knowledge Review Workshop | Y | Y | Y |
| 3 | Discuss DF-C²M² Assessment Tool, process, and objectives | Y | Y | Y |
| 4 | Review Organisational Structure (Mission, Authority, Vision, Quality Policy, etc.) | Y | Y | N |
| 5 | Review of services offered mapped to DF-C²M² Service Catalogue | Y | Y | N |
| 6 | **People Assessment:** Policies, Procedures, SOPs, and Records | Y | Y | N |
|  | Review/witness personnel competency tests & interviews | Y | Y | N |
| 7 | **Process Assessment**: Policies, procedures, SOPs, and records. | Y | Y | N |
|  | Interview selected personnel on Quality Management, Operations, and Technical Processes | Y | Y | N |
| 8 | **Tools and Methods Assessment:** Policies, Procedures, SOPs, and Records | Y | Y | N |
|  | Assessment and witnessing of tool verification and base lining | Y | Y | N |
| 9 | DF-C²M² People Assessment review & findings | Y | Y | N |
| 10 | DF-C²M² Process Assessment review & findings | Y | Y | N |
|  | Assessing compliance with other standards and best practices | Y | Y | N |
| 11 | DF-C²M² Tools Assessment review & findings | Y | Y | N |
| 12 | DF-C²M² Six Steps Model Forensic Readiness Assessment | Y | Y | N |
| 13 | Wrap-up meeting with participants & solicit feedback | Y | Y | N |
| 14 | Create lab assessment report | Y | Y | N |
| 15 | Present Assessment findings to lab | Y | Y | N |
| 16 | Add Assessment findings to benchmark database (spreadsheet) | Y | Y | N |
| 17 | Review & reflect on feedback of DF-C²M² and assessment process | Y | Y | N |

### 7.4.3.1 DF-C$^2$M$^2$ Lab Assessment Step 1 - Organisational Overview

Each lab assessment began with a formal meeting with lab management and a review the lab’s organisational structure, customer base, vision, mission, quality policy, and goals, and the DF-C$^2$M$^2$ goals and objectives were reiterated. Capability Maturity was briefly discussed with the DF-C$^2$M$^2$ core focus on achieving Organisational Capability Maturity via the DF-C$^2$M$^2$ People, Processes, and Tools key domains.

A list of personnel and their roles was recorded. Participants who would assist with the assessment and a more detailed review of the DF-C$^2$M$^2$ were interviewed on key challenges to digital forensics. A sample extract of a transcribed interview is documented in Appendix D – *LAB_A Interview*.

### 7.4.3.2 DF-C$^2$M$^2$ Lab Assessment Step 2 - Review and Mapping of Service to DF-C$^2$M$^2$ Service Catalogue

The initial stage of the assessments was to define and categorise services offered by each lab, within the context of the DF-C$^2$M$^2$, to provide a baseline for the assessment and common criteria for comparison of the two labs, as summarised in Table 31.

Having established a service baseline for the two diverse labs and having mapped their range of services to the Service Catalogue, participants were asked about what they thought the impact and complexity of each service was, and to identify what the underlying prerequisites for the successful delivery of each service were.

The majority of the participants were not able to clearly quantify the impact and complexity of given services, but found the DF-C$^2$M$^2$ Service Catalogue insightful. The participants generally agreed on the default Impact vs. Complexity ratings for each of the DF-C$^2$M$^2$ defined services as initial starting points to be re-assessed at a later stage with more practitioner inputs.

When defining the prerequisites for the delivery of each service, the more experienced practitioners were generally able to identify or summarise the key requirements for delivery of each service, whereas the least experienced participants were not. This unexpected observation helped to identify a new potential use of the DF-C$^2$M$^2$ Service Catalogue – as a valuable learning tool to help train personnel on prerequisite requirements for the delivery of each service in compliance with ISO 17025 and best practice requirements.

Lab #2 was providing a variety of services but had not categorised the services, e.g. Computer Forensics, and its related sub-categories, or created and published a customer-focussed service catalogue as defined within the DF-C$^2$M$^2$.

In contrast, Lab #1 due to the number of years of operation, and ISO 17025 accreditation requirements had a developed a more extensive service catalogue, but had not identified Impact vs. Complexity ratings, nor documented the underlying prerequisites (skills and documented processes) for each service listed. Additionally, the service catalogue was internal and had not been shared it with customers.

Table 31: Summary view of service per lab as per DF-C²M² service catalogue categories

|  | Lab #1 |  |  | Lab #2 |  |  |
|---|---|---|---|---|---|---|
| DF-C²M² Service Category | Service Offered? | Service Introduced In: | Comment | Service Offered? | Service Introduced In: | Comment |
| Computer Forensics (CF) | Y | Dec 2009 | Fully Implemented | Y | Jan 2013 | Fully Implemented * |
| Mobile Device Forensics (MF) | Y | Mar 2010 | Fully Implemented | Y | Jun 2013 | Partially Implemented * |
| Digital Audio Forensics (DAF) | Y | Mar 2011 | Fully Implemented | N | N/A | Not implemented |
| Digital Video Forensics (DVF) | Y | Mar 2012 | Fully Implemented | N | Planned | Not implemented |
| Live & Network Forensics | Y | Sept 2013 | Partially implemented * | N | Planned | Not implemented |
| Cybercrime Analysis | Y | Sept 2013 | Partially implemented * | Y | Aug 2013 | Partially Implemented * |
| Digital Evidence Handling and Support Services | Y | Mar 2010 | Partially implemented * | N | N/A | Partially Implemented * |

**Key: *** Denotes status of service offerings at the time of the assessment.

#### 7.4.3.3 DF-C$^2$M$^2$ Lab Assessment Step 3 - Lab Assessments and Documentation of Findings

Having completed the foundational aspects of the DF-C$^2$M$^2$ introductory and baseline process, each lab was then assessed using the DF-C$^2$M$^2$ Assessment Tool and Body of Knowledge as defined within the DF-C$^2$M$^2$ Framework. The assessment followed the DF-C$^2$M$^2$ Assessment Guidelines:

1. DF-C$^2$M$^2$ People Requirements Assessment
2. DF-C$^2$M$^2$ Process Requirements Assessment
3. DF-C$^2$M$^2$ Tools Requirements Assessment
4. DF-C$^2$M$^2$ Lab Assessment Overall Findings.

The results of the assessment were documented using the DF-C$^2$M$^2$ Assessment Tool, and selected results for Lab #1 are included here as examples in Table 32 and Table 33, with the remainder provided in Appendix E. The findings in the tables are explained and discussed in Section 7.5 next.

#### 7.4.3.4 DF-C$^2$M$^2$ Lab Assessment Step 4 – Present Findings to Lab Managers and Solicit Feedback

A presentation of the DF-C$^2$M$^2$ Assessment, findings, and recommendations was made to the participating lab managers, and their feedback on the DF-C$^2$M$^2$ and the assessment process was solicited. Managers completed a DF-C$^2$M$^2$ evaluation using the DF-C$^2$M$^2$ evaluations form, the details of which are summarised later in this chapter. The DF-C$^2$M$^2$ survey results are included in Appendix C.

Table 32: DF-C²M² assessment ratings lab #1: service catalogue – computer forensics

| Category | Service Description | Service Delivery Group | Dependency on Other Services Identified | Status | % Implemented/ Readiness | Core Or Value Added? |
|---|---|---|---|---|---|---|
| CF1 | Digital Data Extraction from Digital Computer Media | Computer Forensics | n/a | Fully Implemented | 100 | Core |
| CF2 | Digital Forensic Examination & Analysis - Windows | Computer Forensics | Yes | Fully Implemented | 100 | Core |
| CF3 | Digital Forensic Examination & Analysis - Mac OS | Computer Forensics | Yes | Partially Implemented | 50 | Core |
| CF4 | Digital Forensic Examination & Analysis - Unix | Computer Forensics | Yes | Fully Implemented | 50 | Core |
| CF5 | Software Licensing Validation & Anti-Piracy | Computer Forensics | Yes | Fully Implemented | 70 | Value Added |
| CF6 | Decryption and Password Recovery | Computer Forensics | Yes | Partially Implemented | 50 | Core |
| CF7 | Malware Verification and Behavioural Analysis | Computer Forensics | Yes | Partially Implemented | 50 | Core |
| CF8 | Advanced Digital Data Recovery | Computer Forensics | Yes | Fully Implemented | 30 | Value Added |
| CF9 | Computer Evidence Expert Witness Testimony | Computer Forensics | Yes | Fully Implemented | 70 | Core |
| CF10 | Digital Forensics On-Site Response and Seizure | Computer Forensics | Yes | Fully Implemented | 60 | Core |

Table 33: DF-C²M² assessment ratings for lab #1: service catalogue – mobile forensics

| Category | Service Description | Service Delivery Group | Dependency on Other Service Identified | Status | % Implemented/ Readiness | Core or Value-Added? |
|---|---|---|---|---|---|---|
| MHF1 | Digital Data Extraction from Mobile Handsets and SIM Cards | Mobile | Yes | Fully Implemented | 100 | Core |
| MHF2 | Digital Forensic Examination & Analysis of Mobile Handsets & SIM Cards | Mobile | Yes | Fully Implemented | 100 | Core |
| MHF3 | Mobile Handset & SIM Card Data Recovery | Mobile | Yes | Fully Implemented | 100 | Core |
| MHF4 | Digital Data Extraction from GPS Devices | Mobile | Yes | Partially Implemented | 50 | Core |
| MHF5 | Digital Forensic Examination & Analysis of GPS Devices | Mobile | Yes | Partially Implemented | 50 | Core |
| MHF6 | Digital Data Extraction from Digital Media Players and Cameras | Mobile | Yes | Fully Implemented | 100 | Core |
| MHF7 | Mobile Handset Forensics Expert Witness Support and Testimony | Mobile | Yes | Fully Implemented | 70 | Value- Added |
| MHF8 | Mobile Handset Cell Site Analysis | Mobile | N/a | Planned | 53 | Value- Added |

## 7.5 DF-C$^2$M$^2$ LAB ASSESSMENTS

Mapping existing services to the DF-C$^2$M$^2$ Service Catalogue was reviewed in Section 7.4.3.2; it defined a key element as part of the Organisational review (Step 1), and as the basis for the evaluation of:

1. People - Required skills and personnel
2. Process - Required processes and procedures
3. Tools - Required tools and methods
4. Overall Capability Maturity

This section discusses the findings of Lab #1 (an ISO 17025 accredited lab) and those of Lab #2 (a non-accredited lab) respectively beginning with the mapping and compliance assessment of each lab's Service Catalogue followed by the DF-C$^2$M$^2$ People, Processes, and Tools Assessments.

### 7.5.1 Summary of Findings and Observations – Combined Labs

#### 7.5.1.1 Compliance with DF-C$^2$M$^2$ Service Catalogue Requirements

By noting what service each lab had to offer, it was realised that certain services not previously defined within the Service Catalogue had to be categorised, defined, and added as part of the findings of this assessment. Details of the key findings for both Labs #1 and #2 are documented in the section that follows:

##### 7.5.1.1.1 Service Catalogue – Computer Forensics

**Lab #1** - had a comprehensive catalogue of services, given the nature of its business, and the fact that it was a relatively well-established laboratory.

The majority of Lab #1's Computer Forensic services had been successfully implemented. Some value-added services were still being implemented and tested as part of ongoing projects. Overall, Lab #1 met the majority of the requirements of the DF-C$^2$M$^2$ Service Catalogue with:

- 100% of Core Services implemented.
- Overall, over 70% of value-added services having been successfully implemented.

In view of Lab #1's number of years of operations, and its ISO 17025 accreditation, its existing service offerings provided a fairly comprehensive set of services that would cater to the majority of standard examination requests and case types/scenarios.

The implementation of 100% of the Core Services was to be expected for a relatively mature Law Enforcement laboratory. However, as Lab #1 was also a major participant lab during the workshops and reviews, it is also possible that by steering the decision as what should be deemed Core services during the service catalogue workshop, that Lab # 1 participants were simply stating what they were most familiar with, and that perhaps the final determination of what should classified as Core vs. Valued added services requires broader input from a wider range of industry practitioners. This may in some way have skewed the result and classification of what is truly core (essential) versus value-added services in a typical digital forensic law enforcement lab.

**Lab #2** - The services implemented were driven by the nature of its core business, but with plans to expand its range of services based on the Service Catalogue.

In comparison, Lab #2 did not have a defined Service Catalogue, and therefore one was created as part of the organisational review. Lab #2 had implemented the majority of the Computer Forensics service as defined within the Service Catalogue requirements. This added an additional day to the assessment that had not been previously planned for.

Overall, Lab #2 met some of the requirements of the DF-C²M² Service Catalogue (considering that its role is primarily as lab for its academic students) with:

- 70% of Computer Forensics services implemented, and
- 30% of value-added services having been successfully implemented.

#### 7.5.1.1.2 Service Catalogue – Mobile Forensics

**Lab #1** - The majority of Mobile Forensic services had been successfully implemented, with some Value-added services had been planned but were still pending implementation. The existing service offerings provide a comprehensive set of services that would cater for a majority of standard examination requests and case types/scenarios.

Overall, Lab #1 met the majority of the requirements of the DF-C²M² Service Catalogue (considering that it is an established law enforcement laboratory) with:

- 70% of Mobile Forensics implemented.

**Lab #2** – Had implemented the most essential Mobile Forensic services. Value-added services had been planned but were still pending implementation. The existing Service offerings provide an adequate set of services to cover typical service requests and investigation requirements.

Overall, Lab #2 met some of the requirements of the DF-C²M² Service Catalogue with:

- 40% of Mobile Forensics implemented.

#### 7.5.1.1.3 Service Catalogue – Digital Audio & Video Forensics

**Lab #1** – The majority of Digital Audio & Video Forensic services have been successfully implemented, with some Value-added services have been planned but were still pending procurement and implementation. As services mature further in these areas, it may be necessary to separate the two (Digital Audio & Video) into two distinct Service Catalogue groups.

- Overall, over 70% of Digital Audio & Video Forensic-related services had been successfully implemented.

**Lab #2** – did not presently have a business need for Digital Audio and Video Forensics Services, but following the assessment, it was decided by lab management to plan for such services in addition to a related expansion of its present academic curriculum.

#### 7.5.1.1.4 Service Catalogue – Cybercrime Analysis

**Lab #1** – had no defined Service Catalogue for these items. Current ad hoc services were categorised as per the DF-C²M² Service Catalogue for this assessment.

Of the listed services, 45% had been implemented with supporting documentation and procedures at the time of the assessment. A review of Lab #1's strategic roadmap revealed that an expansion along similar lines to the requirements of the Service Catalogue was planned, but not yet implemented. The remainder of services are being provided as and when required, but without the benefit of well-defined and documented technical processes and procedures. Presently, does not meet the majority of the requirements of the DF-C$^2$M$^2$ for Cybercrime analysis, but as noted during the review of the findings Lab #1 stated these requirements were ‘value-add’ and not part of the mandate, but were working towards fulfilling the requirements as part of their overall value-add service offerings.

**Lab #2** – had factored various elements of Cybercrime Analysis within the range of services in support of existing curriculum with no immediate plans to extend these services. Lab #2 had implemented 15% of the related services based on the Service Catalogue.

**Observations:** It was noted that many practitioners had not considered creating a Service Catalogue for Cybercrime Analysis services, nor of categorising services as defined within the DF-C$^2$M$^2$. Likewise, none had considered documenting Impact vs. Complexity analysis for each service.

All agreed that in principle it was a good idea, and would consider implementing it within their organisations, though some did not agree on how services had been labelled or categorised – reinforcing the need to have community-based participation within the DF-C$^2$M$^2$ Framework as a means of helping to standardise certain terms and create a de facto set of service categories for this specialised area or sub-discipline. This is one example where the use of community input into terms, scope and requirements would be beneficial to making the service catalogue more universally acceptable, and assist towards perhaps defining a basic industry wide set of accepted terms and nomenclature.

### 7.5.1.1.5 Service Catalogue – Digital Evidence Tactical Support

**Lab #1 -** The majority of the core Digital Evidence Handling services were still being implemented within the lab, with some value-added services still being implemented.

Overall, Lab #1 meets the majority of the requirements of the DF-C$^2$M$^2$ Service Catalogue; Core Services were partially implemented.

Of the Digital Evidence Tactical Support-related services, 55% had been successfully implemented. No evidence supporting that Digital Evidence Handling & Seizure Training (DETS2) had been provided to external units by Lab #1 at the time of the assessment.

**Lab #2 –** provided facilities and training for 20% of the Core Services in this area.

### 7.5.1.1.6 Service Catalogue Assessment – Overall

**Lab #1**

Services offered were found to be comprehensive, well-planned (with respect to People, Processes, and Tools), but certain value-added services such as Chip-Off and Advanced Disk Repair were not fully implemented as per Lab #1's strategic roadmap at the time of the assessment.

Existing Services were found to be comprehensive and covered Computer Forensics, Mobile Forensics, and Digital Audio-Video Forensics. Value-added services such as Network Forensics and Cybercrime Analysis were at advanced stages of implementation.

Lab #1 had clearly identified service dependencies and prerequisites, and factored these into their service planning, process development, and personnel training paths. Lab #1 met 80% of the requirements of the DF-C$^2$M$^2$ Service Catalogue at the time of the assessment.

**Lab #2**

Existing Services were found to be largely limited to Computer Forensics, with some introduction of Mobile Forensic-related service. As a developing lab, services were continuously being expanded upon, based on curriculum and interest in particular services. As an academic lab, its goal is to provide the most commonly sought-after services that students may expect to find within a commercial or law enforcement laboratory. Lab #2 met 45% of the DF-C$^2$M$^2$ Service Catalogue requirements, which was to be expected given the nature and functions of this largely academic training lab.

Based on the interviews conducted during this assessment, it was felt by the interviewees that the DF-C$^2$M$^2$ standardised Service Catalogue, planning tools, prerequisite planning for each service, and impact ratings system were of great value in helping to standardise the service offering of the lab, and those of participating DF-C$^2$M$^2$ labs for both Lab #1 and Lab #2.

| LAB | SCORE |
|---|---|
| Lab #1 | 4.2 out of 5 |
| Lab #2 | 2.0 out of 5 |

### 7.5.2 Assessment Findings – Six Steps Model - Forensic Readiness

The objective of this stage of the assessment was to evaluate forensic readiness based on the Six Steps Model and to assess participant feedback on the Six Steps Model.

Lab #1 was found to be the most complaint with the Six Steps Model and demonstrated an advanced level of Forensic Readiness. Thus, the assessment results for Lab #1 and the Six Steps Model are illustrated using the Assessment tool. This illustration may also shed some insight on how benchmarking between participant labs can be performed using the assessment for all criteria covered by the DF-C²M² Assessment Tool and Body of Knowledge.

The Assessment tool findings, including the Assessment Tool worksheet, are illustrated below from Table 34 to Table 39 to indicate how the criteria were used, and how the ratings are assigned within the Assessment Tool for Forensic Readiness using the Six Steps Model as an example.

Other completed Assessment Tool worksheets for Lab #1 covering other areas of the assessment are shown in Appendix E.

Table 34: Six steps model – 1. Assessment phase – lab #1

| Category | Description | Score | | |
|---|---|---|---|---|
| | | Level | Rating | Required |
| **A** | **Assessment** | | | |
| A1 | Ability to assess investigator's requirements based on nature of case. | Level 3 - Full Deployment | **3** | **5** |
| A2 | Ability to determine which tools to use based on devices submitted for examination. | Level 4 - Measured & Automated | **4** | **5** |
| A3 | Ability to determine best method and tools to acquire require digital evidence. | Level 4 - Measured & Automated | **4** | **5** |
| A4 | Ability to determine best examiner to handle the case based on training, skills, experience, and qualifications. | Level 3 - Full Deployment | **3** | **5** |
| A5 | Ability to assign an equally competent examiner to act as a technical peer for case review and reference. | Level 3 - Full Deployment | **3** | **5** |
| A6 | Ability to determine what other information may be required from the investigator during initial case review. | Level 3 - Full Deployment | **3** | **5** |
| A7 | Ability to draft a case plan based on the nature of the case, facts known, and what information is required. | Level 2 - Partial Deployment | **3** | **5** |
| A8 | Ability to assess completeness and accuracy of results and report. | Level 3 - Full Deployment | **3** | **5** |
| A9 | Ability to determine any deficiencies in processes, tools, and personnel used and implement corrective actions. | Level 3 - Full Deployment | **3** | **5** |
| A10 | Ability to identify any limitations in findings and caveats that may apply to results. | Level 2 - Partial Deployment | **3** | **5** |

|  |  |  |  |  |
|---|---|---|---|---|
| A11 | Ability to provide a Service Level commitment based on the nature and urgency of the case. | Level 2 –<br>Partial Deployment | **3** | **5** |
| A12 | Ability to determine which cases should not be accepted due to lab's tools, competencies, and processes. | Level 2 –<br>Partial Deployment | **3** | **5** |
| A13 | Ability to determine current and anticipated future technical and personnel requirements (based on trend analysis). | Level 2 –<br>Partial Deployment | **3** | **5** |
| A14 | Ability to obtain legal counsel to help determine any limitations (exceptions) to investigation. | Level 2 –<br>Partial Deployment | **3** | **5** |
| A15 | Ability to conduct a risk assessment with regards to personnel safety onsite. | Level 3 –<br>Full Deployment | **3** | **5** |
| A16 | Ability to conduct a risk assessment with regards to personnel safety onsite and to counter these where possible. | Level 3 –<br>Full Deployment | **3** | **5** |
| A17 | Ability to determine health and safety factors when handling evidence specific to a case, e.g. contaminated by bio-hazards/chemical substances. | Level 4 –<br>Measured & Automated | **4** | **5** |
| A18 | Ability to determine if requested services/examination are defined within current Service Catalogue, technical procedures, and staff capabilities. | Level 3 –<br>Full Deployment | **4** | **5** |
| **Total Score** |  |  | **58** | **90** |
| **Maturity Level Average** |  | **Level 3 - Full Deployment** | **3.22** |  |

#### 7.5.2.1 Assessment Phase - Assessor’s Comments

There is an opportunity to further improve the case assessment and planning capabilities, and thereby help to improve the overall case and operational efficiency.

The collective expertise of the lab team could be better utilised by performing initial case planning and assessment by competent/experienced personnel mandatory for all cases.

The requirement for an internal Knowledge Base was identified as a key requirement by lab personnel – a requirement that would be addressed by the DF-C²M² and would further enhance this capability within the lab, and help to improve the overall expertise of examiners. The knowledge base like that proposed by the DF-C²M² should include case type guidelines/checklists, as well as technology-specific references, e.g. Investigating VoIP abuse cases.

Lab #2 – The requirements were defined within the curricula documentation and assignments. This lab would benefit from the use of the Assessment workflows for inclusion in lab of processes and guidelines.

| LAB | SCORE |
|---|---|
| Lab #1 | 3.22 out of 5 |
| Lab #2 | 1.83 out of 5 |

Table 35: Six steps model – 2. Collection phase – lab #1

| Category | Description | Score | | |
|---|---|---|---|---|
| | | Level | Rating | Required |
| C | Collection | | | |
| C1 | Able to effectively mobilise digital forensics/incident response team (internal & external). | Level 2 - Partial Deployment | 2 | 5 |
| C2 | Able to effectively handle and preserve evidence associated with the case/incident. | Level 4 - Measured & Automated | 4 | 5 |
| C3 | Able to accurately identify sources of digital evidence related to the incident/case. | Level 3 - Full Deployment | 3 | 5 |
| C4 | Able to collect evidence both covertly and overtly in a timely and effective manner (on site). | Level 2 - Partial Deployment | 2 | 5 |
| C5 | Able to collect online evidence both covertly and overtly in a timely and effective manner (remotely). | Level 2 - Partial Deployment | 2 | 5 |
| C6 | Have required tools and skills to correctly disassemble and re-assemble devices as part of evidence acquisition process. | Level 4 - Measured & Automated | 4 | 5 |
| C7 | Has implemented well-defined and tested digital evidence logging, capturing, securing, and retention policies and procedures. | Level 4 - Measured & Automated | 4 | 5 |
| C8 | Has well-defined policies to determine how best to preserve digital evidence based on case type and nature of digital evidence sought. | Level 5 - Continuously Improving | 5 | 5 |
| C9 | Able to conduct in lab triage and prioritisation of devices related to a single case. | Level 2 - Partial Deployment | 2 | 5 |
| C10 | Able to conduct on-site triage to identify possible sources of evidence related to case. | Level 2 - Partial Deployment | 2 | 5 |
| C11 | Able to mobilise first responder team in a timely manner to assist with digital evidence collection. | Level 2 - Partial Deployment | 2 | 5 |
| C12 | Able to mobilise first responder team in a timely manner to assist with on-site digital evidence acquisition. | Level 2 - Partial Deployment | 2 | 5 |

| | | | | |
|---|---|---|---|---|
| C13 | Has a well-defined contingency plan to summon additional trained first responders when responding to a large-scale incident (if required). | Level 1 - Documented Process | **1** | **5** |
| C14 | Has the required and sufficient quantity of tools to assist with efficient digital evidence capture and documentation. | Level 4 - Measured & Automated | **4** | **5** |
| C15 | Has streamlined internal processes to maximise collection efforts with minimal delay and loss of potential evidence. | Level 2 - Partial Deployment | **2** | **5** |
| C16 | Has required tools and skills to assist with live evidence capture from running systems that cannot be taken offline or physically seized. | Level 2 - Partial Deployment | **2** | **5** |
| C17 | Has well-defined policies to determine how best to collect and preserve digital evidence from mobile phones. | Level 3 - Full Deployment | **3** | **5** |
| C18 | Has well-defined policies to determine how best to collect and preserve digital evidence from computers. | Level 3 - Full Deployment | **3** | **5** |
| C19 | Has well-defined policies to determine how best to collect and preserve digital evidence from CCTV digital video recorders. | Level 3 - Full Deployment | **3** | **5** |
| C20 | Has well-defined policies to determine how best to collect and preserve digital evidence from network devices. | Level 2 - Partial Deployment | **2** | **5** |
| C21 | Has well-defined policies to determine how best to collect and preserve digital evidence from online/cloud storage systems. | Level 2 - Partial Deployment | **2** | **5** |
| C22 | Has established process and channels of communication to assist with obtaining online activity records from service providers. | Level 1 - Documented Process | **1** | **5** |
| C23 | First responders have required tools/support to conduct on-site risk assessment to minimise potential of evidence loss, damage (volatility, etc.). | Level 2 - Partial Deployment | **2** | **5** |
| C24 | Procedures of evidence collection and acquisition provide sufficient and detailed documentation of steps, processes, and personnel involved. | Level 4 - Measured & Automated | **4** | **5** |
| C25 | Digital evidence collection processes at a minimum ensure ACPO's core principles (and any local and state legal requirements). | Level 4 - Measured & Automated | **4** | **5** |
| C26 | Processes and tools used conform with ISO 27037 standards (i.e. ISO 23027 compliant), e.g. regarding labelling, packaging, and transportation. | Level 3 - Full Deployment | **3** | **5** |
| **Total Score** | | | **70** | **130** |
| **Maturity Level Average** | | **Level 2 - Partial Deployment** | **2.69** | |

#### 7.5.2.2 Assessor's Comment – Six Steps Model - Collection Phase

**Lab #1 -** The assessment uncovered several gaps in the current service capability regarding forensic evidence collection, which although planned for through certain projects such as Live and Network Forensic, have not been implemented.

Presently, very little evidence collection from crime scenes is done directly by the lab personnel, even though the facility's tools, personnel, and training have been accounted for. Evidence handing and imaging processes within the lab are well-defined and documented.

**Lab #2 -** did not participate in evidence collection, and personnel who manned the lab on a full-time basis were interviewed and assessed. Partially implemented and documented.

| LAB | SCORE |
|---|---|
| Lab #1 | 2.69 out of 5 |
| Lab #2 | 1.31 out of 5 |

Table 36: Six steps model – 3. Examination phase – lab #1

| Category | Description | Score | | |
|---|---|---|---|---|
| | | Level | Rating | Required |
| **E** | **Examination** | | | |
| E1 | Established tools and processes used for digital forensic examination. | Level 4 - Measured & Automated | **4** | **5** |
| E2 | Examiners are trained and externally proficiency tested in all areas of examination the lab is required to perform. | Level 2 – Partial Deployment | **2** | **5** |
| E3 | Examination processes/methods used are documented and are auditable, and the results are verifiable as per requirements of ISO 17025. | Level 5 - Continuously Improving | **5** | **5** |
| E4 | Examination process includes technical peer review of all work and any findings. | Level 4 - Measured & Automated | **4** | **5** |
| E5 | Examination process is well-documented and periodically updated/reviewed. | Level 5 - Continuously Improving | **5** | **5** |
| E6 | Examination skills cover a majority of services defined with the Service Catalogue. | Level 3 - Full Deployment | **3** | **5** |
| E7 | Examiners are competency tested on all examination types are required to perform at least annually. | Level 3 - Full Deployment | **3** | **5** |
| E8 | Examiners have a clearly defined code of conduct, roles, and job descriptions. | Level 3 - Full Deployment | **3** | **5** |
| E9 | Examination process begins with verification of tools. | Level 4 - Measured & Automated | **4** | **5** |
| E10 | Examinations will not (generally) affect the original evidence (mobile phones may be an exception). | Level 4 - Measured & Automated | **4** | **5** |
| E11 | Examinations for various device types, e.g. mobile phone, computer, or CCTV, have well-defined processes, tools, and evidence handling procedures. | Level 3 - Full Deployment | **3** | **5** |
| E12 | Examinations and processes used are documented in case notes by the examiner. | Level 4 - Measured & Automated | **4** | **5** |
| E13 | All examinations are subject to technical and administrative peer review by suitably qualified personnel. | Level 5 - Continuously Improving | **5** | **5** |

| | | | | |
|---|---|---|---|---|
| E14 | Examinations are limited to the scope of the investigation and evidence sought (unless otherwise stated by a competent legal authority). | Level 3 - Full Deployment | **3** | **5** |
| E15 | Any acquired and any derivative evidence (including reports and case notes) are securely preserved for the minimum legally stipulated period and secured with suitable access controls. | Level 3 - Full Deployment | **3** | **5** |
| E16 | Examination types are classified based on nature of services requested and estimated levels of complexity (e.g. Service Level 1 is basic data extraction). | Level 1 - Documented | **1** | **5** |
| E17 | Examinations are given Service Level Targets based on the number of devices and what information is required. Service Levels are tracked and deviations remediated. | Level 2 - Partial Deployment | **2** | **5** |
| E18 | Subcontracting of any examinations beyond the scope of capability of the lab is well-defined and can only be issued to suitably qualified sub-contractors with customer consent | Level 3 - Full Deployment | **3** | **5** |
| E19 | Any examinations that may affect the integrity of the evidence or may result in damage to the original device can only be undertaken after customer written consent. | Level 3 - Full Deployment | **3** | **5** |
| E20 | Team and examiner efficiency is tracked based on Service Level conformance and case complexity. | Level 2 - Partial Deployment | **2** | **5** |
| E21 | Examination progress checklists are used for common types of examination requests. | Level 2 - Partial Deployment | **2** | **5** |
| E22 | Only validated tools and methods may be used for examinations without requesting a Standard Deviation request from the lab manager and customer. | Level 3 - Full Deployment | **3** | **5** |
| E23 | Case work during examinations is backed up regularly to prevent data loss during examination process. | Level 4 - Measured & Automated | **4** | **5** |
| E24 | All devices to be examined are uniquely documented and photographed. | Level 4 - Measured & Automated | **4** | **5** |
| E25 | The use of trusted external technical references is permitted during examinations. | Level 4 - Measured & Automated | **4** | **5** |
| E26 | An internal knowledge base of systems, tools, and methods (including third-party references) is maintained and readily accessible by authorised personnel. | Level 1 - Documented | **1** | **5** |
| E27 | Customer is regularly informed of any progress during the ongoing examination. | Level 3 - Full Deployment | **3** | **5** |
| E28 | All examinations must be accompanied by a Letter of Authorisation (Warrant) that specifically states what is to be examined and for what types of evidence. | Level 4 - Measured & Automated | **4** | **5** |
| E29 | Multiple examiners may work on a single case; each will be assigned specific items to examine and report to the lead examiner assigned to the case. | Level 3 - Full Deployment | **3** | **5** |
| E30 | Examination may be re-assigned to another examiner, if required, using a documented case hand-over and approval process. | Level 3 - Full Deployment | **3** | **5** |
| | **Total Score** | | **97** | **150** |
| | **Maturity Level Average** | **Level 3 - Full Deployment** | **3.23** | |

#### 7.5.2.3 Assessor's Comment – Six Steps Model – Examination Phase

**Lab #1 -** Overall, the vast majority of the examination processes and practices were found to be sound and uniformly applied. Opportunities for improvement exist in a number of areas including:

1. **E11: - "Examinations for various devices types, e.g. mobile phone, computer, or CCTV, have well-defined processes, tools, and evidence handling procedures."**
   Sample finding notes for E11 are: it was determined through interviews of processes used for video examinations that although processes for digital video/CCTV data extraction and examination have been created, the process manual is followed inconsistently by examiners, and that Digital Video Examination has not yet been added to the ISO 17025 Scope of Accreditation. Video cases account for a significant percentage of cases processed by the lab, and therefore compliance with the Video Technical Manual (policies and processes) is vital. Accordingly, efforts towards expanding the current ISO 17025 Scope of Accreditation should be made.
2. **E2: - "Examiners are trained and externally proficiency tested in all areas of examination they are required to perform."** – The lack of external proficiency tests and inter-lab comparison of results has been previously documented within this assessment.

**Lab # 2 –** defined with curricula to some degree. Needs to be more structured and aligned to best practices.

| LAB | SCORE |
|---|---|
| Lab #1 | 3.23 out of 5 |
| Lab #2 | 1.40 out of 5 |

Table 37: Six steps model – 4. Analysis phase – lab #1

| Category | Description | Score | | |
|---|---|---|---|---|
| | | Level | Rating | Required |
| AN | Analysis | | | |
| AN1 | Ability to perform a detailed analysis of evidence in relation to reported incident/case. | Level 3 - Full Deployment | 3 | 5 |
| AN2 | Ability to perform through forensic examinations of available evidence relating to the case. | Level 3 - Full Deployment | 3 | 5 |
| AN3 | Provide support and feedback to investigators in support of ongoing investigations. | Level 3 - Full Deployment | 3 | 5 |
| AN4 | Analysis and findings to be based on verifiable facts and not opinions. | Level 3 - Full Deployment | 3 | 5 |
| AN5 | Analysis process and any supporting documents/tools have been adequately tested and referenced in case notes. | Level 5 - Continuously Improving | 5 | 5 |
| AN6 | Analysis may be able to provide remediation report on how to address certain issues that may have resulted in the incident (relates to Information Security breaches). | Level 1 - Documented Process | 1 | 5 |
| AN7 | Analysis should also provide input for service/methods improvement (where possible) as part of case audit/review. | Level 5 - Continuously Improving | 5 | 5 |
| AN8 | Examiners should be aware that any analysis process and results should be presentable in a court, if required. | Level 4 - Measured & Automated | 4 | 5 |
| AN9 | Analysis process and results are subjected to a technical and administrative peer review by suitably qualified personnel (which may include subject matter experts and investigators). | Level 5 - Continuously Improving | 5 | 5 |
| AN10 | Analysis should also identify any limitations of the collection, examination, and analysis processes used. | Level 3 - Full Deployment | 3 | 5 |
| | **Total Score** | | **35** | **50** |
| | **Maturity Level Average** | **Level 3 - Full Deployment** | **3.50** | |

#### 7.5.2.4 Assessor’s Comment – Six Steps Model - Analysis Phase

**Lab #1 -** Overall, the analysis processes (including technical peer review) were found to be sound, but could further be improved by addressing some deficits highlighted in the Assessment Phase of the Six Steps Model (mentioned earlier).

Item AN6: “Analysis may be able to provide remediation report on how to address certain issues that may have resulted in the incident (relates to Information Security breaches).” This was to be covered within the lab documentation, but other than a few isolated cases, in general the affected organisation/victims of incidents such as hacking do not benefit from the expertise of the lab personnel in receiving remediation advice.

**Lab #2** – The analysis requirements were found to be adequate, with room for improvement and a more structured approach to Analysis.

| LAB | SCORE |
|---|---|
| Lab #1 | 3.5 out of 5 |
| Lab #2 | 2.0 out of 5 |

Table 38: Six steps model – 5. Reporting phase – lab #1

| Category | Description | Score | | |
|---|---|---|---|---|
| | | Level | Rating | Required |
| **R** | **Reporting** | | | |
| R1 | Identify the requirements for investigation. | Level 3 - Full Deployment | 3 | 5 |
| R2 | Determine the legal requirements for examination. | Level 3 - Full Deployment | 3 | 5 |
| R3 | Identify the technical tools and processes used. | Level 4 - Measured & Automated | 4 | 5 |
| R4 | Reports should be written in non-technical terms (wherever possible) and include a glossary. | Level 3 - Full Deployment | 3 | 5 |
| R5 | Reports should identify date items where received, date examined, and date of report issue. | Level 5 - Continuously Improving | 5 | 5 |
| R6 | All examiners (primary and any secondary examiners) who worked on the examination, analysis, and reporting should be clearly identified in the report. | Level 2 – Partial Deployment | 2 | 5 |
| R7 | Opinions of the examiner and investigator are not permitted to be included in the report. | Level 5 - Continuously Improving | 5 | 5 |
| R8 | Reports should be factual, verifiable, and unbiased. | Level 5 - Continuously Improving | 5 | 5 |
| R9 | All reports are to be duly signed by examiner(s) and lab manager. | Level 5 - Continuously Improving | 5 | 5 |
| R10 | Each page of the report is to be stamped for authenticity. | Level 5 - Continuously Improving | 5 | 5 |
| R11 | All reports should have a confidentiality label and case number assigned to each page. | Level 5 - Continuously Improving | 5 | 5 |
| R12 | Any subsequent reports, e.g. for additional items examined or requested, must be labelled and supplementary to the original report dated (dd-mm-yyyy). | Level 4 - Measured & Automated | 4 | 5 |
| | **Total Score** | | **49** | **60** |
| | **Maturity Level Average** | **Level 4 - Measured & Automated** | **4.08** | |

### 7.5.2.5 Assessor’s Comment – Six Steps Model – Reporting Phase

**Lab #1 -** Overall, the reporting processes were found to be sound with detailed, clear, and unambiguous reports issued by the lab. One limitation identified was that no glossary of commonly used technical terms and conditions is included with the report. This may result in examiners having to spend additional time explaining these terms to investigators and prosecutors, and this may be counterproductive to overall examiner and lab efficiency.

Consistent technical peer reviews (by Senior Examiners) of all reports and findings have provided an effective framework to identify and address any potential issues/ambiguities in reports.

**Lab #2** – Required as part of assignments, but no controls to ensure that this is fully implemented by the examiners (students) prior to submission of the final work product to faculty members acting as the customers in this scenario.

| LAB | SCORE |
|---|---|
| Lab #1 | 4.08 out of 5 |
| Lab #2 | 2.0 out of 5 |

Table 39: Six steps model – 6. Review phase – lab #1

| Category | Description | Score | | |
|---|---|---|---|---|
| | | Level | Rating | Required |
| **RV** | **Review** | | | |
| RV1 | Technical peer review of examination process, analysis, and findings conducted for each case. | Level 4 - Measured & Automated | **4** | **5** |
| RV2 | Administrative peer review of process compliance is conducted for each case. | Level 4 - Measured & Automated | **4** | **5** |
| RV3 | Case report reviewed and explained to the customer. | Level 2 – Partial Deployment | **2** | **5** |
| RV4 | Customer feedback of examination timeliness; report to be solicited and documented upon completion of each case. | Level 3- Full Deployment | **3** | **5** |
| RV5 | Each new case type (e.g. new device) should be treated as a lessons learnt opportunity and new knowledge gained related to tools or processes should be shared with other examiners via Knowledge Base. | Level 2 - Partial Deployment | **2** | **5** |
| RV6 | Any areas of improvement or shortcomings should be identified and addressed via corrective/preventative actions. | Level 3 – Full Deployment | **3** | **5** |
| | **Total Score** | | **18** | **30** |
| | **Maturity Level Average** | **Level 3 - Full Deployment** | **3.00** | |

#### 7.5.2.6 Assessor's Comment – Six Steps Model – Review Phase

**Lab #1 -** Overall, sound policies and procedures have been defined and implemented. Opportunities for improvement in the Six Steps case review phase exist mainly as they relate to the following items: RV5- "Each new case type (e.g. new device) should be treated as a lessons learnt opportunity and new knowledge gained related to tools or processes should be shared with other examiners via Knowledge Base.", and RV3:- "Case report reviewed and explained to the customer".

Given the requirement to conduct reviews from a lessons learnt perspective for each new device type/case type, it was determined during the assessment that this was mostly still being done in an ad hoc manner by a few individuals, and the knowledge gained was not being shared formally via a knowledge base or regular case review meetings with all personnel. Implementing these procedures formally as defined within the lab's manuals will serve to help improve the lab's overall collective knowledge and experience.

**Lab #2** – Not sufficiently defined from an examiner's (student) perspective. The academic criteria used to evaluate reports are outside the scope of the DF-C$^2$M$^2$.

| LAB | SCORE |
|---|---|
| Lab #1 | 3 out of 5 |
| Lab #2 | 1 out of 5 |

#### 7.5.2.7 Overall DF-C$^2$M$^2$ Six Steps Model Readiness Process Maturity Assessment Results – Lab #1 vs. Lab #2:

**Lab #1** rated well in the majority of areas, showing process maturity in several areas and increased proficiency in all areas, but as Lab #1 is not solely responsible for the collection and handling of digital evidence at crime scenes, and in view of the fact that most departments have not been trained in digital evidence handling, there is significant room for improvement in comparison with the DF-C$^2$M$^2$ requirements for the organisation as a whole. Within the scope of the DF-C$^2$M$^2$ Model, Lab #1 meets all of the DF-C$^2$M$^2$ requirements.

**Lab #1:** Overall, Lab #1 showed an advanced level of forensic readiness capability considering that it has been effectively in operation for just 3 years, and achieved a score of 3.28 out of 5 (Fully Deployed based on the Maturity Model).

In summary, Lab #1 has set a high standard across the board, but would benefit from improvements in areas related to process automation, advanced skills development and training, and greater benefits from a digital forensics-specific set framework than what is currently available.

**Lab #2**: Within the scope of the DF-C$^2$M$^2$ Model, Lab #2 meets some of the DF-C$^2$M$^2$ requirements.

**Lab #2:** As a newly established lab, Lab #2 showed good potential as a new lab looking to implement international standards and best practices.  It was initially designed to cater to students attending courses, but later realised the potential of expanding its services and customer base, and implementing international standards.

Lab #2 achieved a score of 1.59 out of 5 (Level 1 - Documented Process for Forensic Readiness). Figure 27 illustrates the actual versus required ratings for Lab #2 for each area of the Six Steps Model Assessment based on the Assessment Tool.

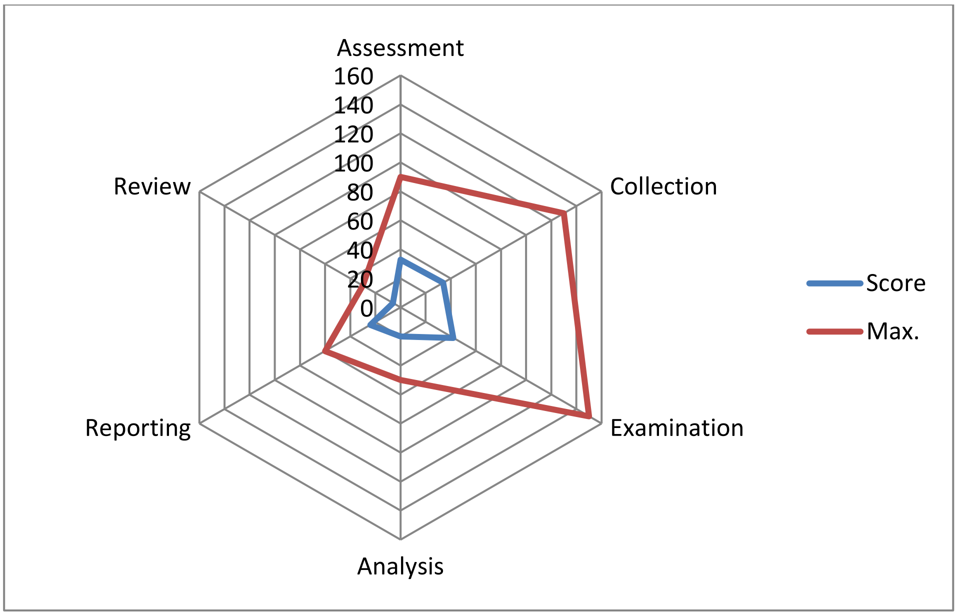


**Figure 27: Lab #2 – Six steps model actual vs. required**

Table 40 shows the Overall DF-C²M² Six Steps Model Readiness Process Maturity Assessment Results for Lab #1 vs. Lab #2.

Table 40: Overall DF-C²M² six steps model readiness process maturity assessment results – lab #1 vs. lab #2.

| DF-C$^2$M$^2$ **Category** | **Max Score** | **Lab #1 Score** | **Lab #1 CMM Rating** | **Lab #1 Maturity Level** | **Lab #2 Score** | **Lab #2 CMM Rating** | **Lab #2 Maturity Level** |
|---|---|---|---|---|---|---|---|
| 1. Assessment | 90 | 58 | 3.22 | Level 3 - Full Deployment | 33 | 1.83 | Level 1 - Documented Process |
| 2. Collection | 130 | 70 | 2.69 | Level 2 - Partial Deployment | 34 | 1.31 | Level 1 - Documented Process |
| 3. Examination | 150 | 97 | 3.23 | Level 3 - Full Deployment | 42 | 1.40 | Level 1 - Documented Process |
| 4. Analysis | 50 | 35 | 3.50 | Level 3 - Full Deployment | 20 | 2.0 | Level 2 - Partial Deployment |
| 5. Reporting | 60 | 49 | 4.08 | Level 4 - Measured & Automated | 24 | 2.0 | Level 2 - Partial Deployment |
| 6. Review | 30 | 18 | 3.0 | Level 3 - Full Deployment | 6 | 1.0 | Level 1 - Documented Process |
| **Overall Score** | **510** | **327** | **3.28** | **Level 3 - Full Deployment** | **159** | **1.59** | **Level 1 - Documented Process** |

## 7.6 DF-C$^2$M$^2$ ASSESSMENT OF THE PEOPLE DOMAIN - ASSESSING COMPETENCY OF DIGITAL FORENSICS PERSONNEL

Within the specialist area of Digital Forensics, four specific technical job roles have been identified and job descriptions drafted for use within the DF-C$^2$M$^2$. These four key technical roles defined within the DF-C$^2$M$^2$ are:

1. Digital Forensic Trainee
2. Digital Forensic Engineer
3. Digital Forensics Examiner
4. Digital Forensics Specialist

Together with a review of training plans and progress for each technical member of the staff, as well as witnessing several competency tests and reviewing the results, the following results are based on overall competency and skills assessment for select representatives of the team.

Note: These roles were mostly found to be not applicable to Lab #2's current academic lab setup at present, and therefore although the creation of these roles is part of Lab #2's goal, these roles did not exist within Lab #2 at the time of the assessment. Thus, the role of Trainee was introduced to cover the majority of Lab #2's users who would initially be entry-level students, possibly becoming Forensic Engineers at the later stages of their academic education.

### 7.6.1 People Domain - Lab Assessment and Findings using DF-C$^2$M$^2$

**Lab #1** – As a well-established and accredited lab, Lab #1 had a complete complement of personnel covering all personnel roles within the DF-C$^2$M$^2$, and therefore serves as an ideal candidate through which the DF-C$^2$M$^2$ People component and Capability Maturity could be tested. Performance statistics for personnel were largely based on the volume of work completed over a given period, the number of devices processed, and training received.

From a People perspective, **Lab #2** was staffed by a small, dedicated, and experienced team of personnel, supplemented with transient students who used the facility as part of their studies and research projects.

This initially posed a challenge for the DF-C$^2$M$^2$, as this model was designed to assess personnel of a more permanent nature, and the various People elements of DF-C$^2$M$^2$ Training, and Coaching manuals, were geared towards the training and mentoring of personnel over a period of at least a year to fulfil some of the DF-C$^2$M$^2$ lower-rung job profiles.

This, therefore, meant that these students would have to be classified as Trainees, and with the more senior and experienced students possibly as Forensic Engineers - all working under the supervision of more experienced full-time lab personnel as per the requirements defined within the DF-C$^2$M$^2$.

Essentially, this meant that the students, who were also users of the laboratory, could not be fully assessed to address the People elements of the DF-C$^2$M$^2$, but they could be involved in the review of the model and its utility on. Full-time personnel within the lab, on the other hand, would be assessed.

Within Lab #2, People Capability Maturity was not presently factored into any aspects of the lab’s policies or strategic requirements.

#### 7.6.1.1 People Domain - Competency of Personnel

All personnel training records were reviewed, as were recent competency tests. Specific tasks were witnessed to check for competency and compliance, and overall, all roles proved to be competent and in some areas highly proficient at performing the required tasks designated for each role.

**Lab #1**: has a mature, well-structured, and well-planned training and mentoring model that address the core requirements for each of the technical and non-technical roles within the lab. Engineers and Examiners had previously been tested and have demonstrated their competency in all required areas.

External proficiency tests were conducted at least annually, but focussed on Computer Forensics, and no external proficiency test or inter-lab comparisons of results were conducted for digital video or mobile phone forensics due to the nonexistence of Mobile Forensic proficiency tests at the time.

As part of the DF-C$^{2}$M$^{2}$'s Value proposition, this model would automatically cater to these requirements and provide a pool of accredited labs with which to conduct inter-lab comparison of results, if required.

Based on interviews conducted during this assessment, it was felt by the interviewees that the DF-C$^{2}$M$^{2}$ Knowledge Base and Technical Workflows would help to enhance the current in-house training and mentoring that is conducted, and many saw great value in the idea of collaborative peer reviews and best practices to help streamline processes in line with what would be internally accepted best practices under the DF-C$^{2}$M$^{2}$.

**Lab #2**: has a well-structured training programme that addresses the core requirements of the technical roles within the lab as part of its academic curricula and internal processes. The majority of the training, however, was focussed on technical processes, with little or no training on Quality Management and operational lab requirements. As an academic institution following established academic curricula lab - whose primary purpose is to train students - this is not unusual. It should be noted that DF-C$^2$M$^2$ is primarily designed to assist accredited and new labs wishing to be accredited with maintaining accreditation and achieving capability maturity. Labs that do not wish to be accredited will still benefit from DF-C$^2$M$^2$ through the assessment tool results, and body of knowledge, which if fully implemented would facilitate a lab to achieve accreditation relatively cost-effectively.

The DF-C$^2$M$^2$ assessment tool enables assessments of labs based on the body of knowledge, ISO 17025, ASCLD-LAB and CMM requirements and best practices, Labs that choose not to implement certain parts of the above foundational elements will therefore not fare well in these assessments.

Personnel staffing the lab, and a select set of students, were assessed and were mostly found to have demonstrated their competency in all required areas. No external proficiency tests were conducted.

**Overall:** Based on interviews conducted during this assessment, it was felt by the interviewees in both labs that the DF-C$^2$M$^2$ Six Steps Model and Knowledge Base (technical workflows, processes) would help to enhance the current in-house training and mentoring that is conducted, and many saw great value in the idea of collaborative peer reviews and best practices to help streamline processes in line with what would be internally accepted best practices under the DF-C$^2$M$^2$.

#### 7.6.1.1.1 Participant Feedback on People Assessment from Lab #1

The witnessing of tests provided some insight that was used for the P-CMM assessment of personnel, but it also came to light during this process when reviewing Service Levels within each lab, that having various personnel who rated highly on the P-CMM element was not an indication of actual performance for that individual.

It was possible that an individual would rate highly in the P-CMM assessment and yet have a poor record of compliance with service levels within the lab. It therefore became apparent at this stage that P-CMM elements need to be combined with Service Level conformance in order to truly assess and gauge individual’s actual P-CMM rating versus their overall efficiency over a period of time to determine their average P-CMM rating.

This theoretically could be achieved on an ongoing basis through the use of some form of performance monitoring and tracking tool (spreadsheet) - tracking actual utilisation, conformance with service level targets, and more granular details on for example an individual’s average time taken to complete a specific task for example imaging and processing a 500GB hard drive. Such as system would give a more accurate P-CMM assessment of an individual over a given time period e.g. 12 months. It would also enable benchmarking between individuals within the same team, performing largely the same types of tasks and examinations.

To that end, a performance service level and rating tracking spreadsheet was created to help provide a more realistic rating for personnel, based on statistics from their previous case work history. The tool was demonstrated using sample, but insufficient real data was available to determine its weaknesses and long-term viability as part of the assessments.

#### 7.6.1.1.2 Participant Feedback on People Assessment from Lab #2

The faculty head of the department realised the need for emerging digital forensic students at their facility to learn both the technical aspects of digital forensic examinations, but also to learn the procedural and quality management aspects at the same time. Thus, the interest in assessing the status versus that of an accredited ISO 17025 laboratory and the DF-C$^2$M$^2$ was of special interest to the faculty. The goal of Lab #2 was eventually to include DF-C$^2$M$^2$ processes, Knowledge Base, and methods as part of the lab's standard student operations and to supplement existing curricula with information on lab processes and standards. This idea is being explored by the faculty at this time.

#### 7.6.1.1.3 Observations

Personnel proficiency without having a series of previous case records to analyse for completeness, timeliness, etc., was difficult. The assumption at the start of the assessment was that such data and case history would be available for review for both labs. Whilst Lab #1 had an archive of historical data and case work available for review, Lab #2 did not. This, therefore, eliminated Lab #2 from much of this section of the assessment.

### 7.6.2 Digital Forensic Engineer Lab #1 – Sample Summary Report & Comments

Overall, the assessed individual (trainee Forensic Engineer) was found to possess the minimum skill requirements to perform the duties defined within the job description. The individual had been with the lab for less than six months, and certain areas related to "soft skills" and advanced subjects required further attention and remediation at the time of the assessment, as these were below the lab's skills and competency requirements. In general, the requirements for a labs skills and competency are defined in accordance with ISO 17025/ASCLD-LAB criteria, and is also defined within the DF-C$^2$M$^2$ assessment tool and DF-C$^2$M$^2$ competency test requirements.

The individual works under supervision until such time as they have met all of the requirements, and is officially competency re-tested in all areas, and issued an internal Certificate as a Forensic Engineer authorised to perform Machine Disassembly, Digital Media Imaging, Data Recovery, and assist examiners with pre-processing tasks (under Examiner supervision).

Based on the other assessment results reviewed for other Forensic Examiners, the majority of those Forensic Engineers who had been in the roles for more than 6 to 9 months had exceeded all of the requirements found to be applicable to all of the Forensic Engineers with LAB #1.

The following table, Table 41, is the Assessment Tool assessment results for a Forensic Engineer taken from the Lab #1 People Assessment. The actual versus required scores for the position of Forensic Engineer are also represented in Figure 28.

### Table 41: People domain - digital forensic engineer – lab #1

| | | | Skill Level | Score | Required | Max. |
|---|---|---|---|---|---|---|
| IT Fundamentals | 1 | Computer Fundamentals (A+) | Level 5 - Expert | 5 | 3 | 5 |
| | 2 | Network Fundamentals (Network+) | Level 3 - Competent | 3 | 3 | 5 |
| | 3 | Security Fundamentals (Security+) | Level 3 - Competent | 3 | 3 | 5 |
| Forensics Introduction | 4 | APCO Digital Forensic Principles | Level 4 - Proficient | 4 | 3 | 5 |
| | 5 | Media Wiping & Verification | Level 5 - Expert | 5 | 3 | 5 |
| | 6 | Media Imaging & Verification | Level 5 - Expert | 5 | 3 | 5 |
| | 7 | Forensics Workstation Operation & Maintenance | Level 4 - Proficient | 4 | 3 | 5 |
| | 8 | Ghost Process and Rebuild (Verification) | Level 5 - Expert | 5 | 3 | 5 |
| | 9 | Media Imaging: Dossier Operation | Level 5 - Expert | 5 | 3 | 5 |
| | 10 | Media Imaging: Omniwipe Operation | Level 4 - Proficient | 4 | 3 | 5 |
| | 11 | Bulk Media Imaging: Rimage Operation | Level 4 - Proficient | 4 | 3 | 5 |
| | 12 | Write-Blocker Usage and Testing | Level 4 - Proficient | 4 | 3 | 5 |
| Forensics Fundamentals | 13 | File System Analysis | Level 3 - Competent | 3 | 3 | 5 |
| | 14 | Data Recovery Tools and Process | Level 3 - Competent | 3 | 3 | 5 |
| | 15 | Windows O/S Artefacts | Level 4 - Proficient | 4 | 3 | 5 |
| | 16 | Internet Artefacts | Level 4 - Proficient | 4 | 3 | 5 |
| | 17 | File Analysis | Level 2 - Beginner | 2 | 3 | 5 |
| | 18 | Documentation and Case Work | Level 4 - Proficient | 4 | 3 | 5 |
| Mobile Forensics | 19 | Mobile Forensics Principles 101 | Level 2 - Beginner | 2 | 3 | 5 |
| | 20 | SIM Card Analysis | Level 4 - Proficient | 4 | 3 | 5 |
| | 21 | Mobile Handset Analysis | Level 3 - Competent | 3 | 3 | 5 |
| | 22 | Using XRY for Logical Extraction | Level 4 - Proficient | 4 | 3 | 5 |
| | 23 | Using UFED for Logical Extraction | Level 3 - Competent | 3 | 3 | 5 |
| | 24 | Imaging Mobile Handsets | Level 3 - Competent | 3 | 3 | 5 |
| Primary Forensic Tools | 25 | FTK - Fundamentals | Level 4 - Proficient | 4 | 3 | 5 |
| | 26 | PRTK - Fundamentals | Level 4 - Proficient | 4 | 3 | 5 |

| | | | | | | |
|---|---|---|---|---|---|---|
| | 27 | Encase - Fundamentals | Level 4 - Proficient | **4** | **3** | **5** |
| | 28 | NetAnalysis - Fundamentals | Level 4 - Proficient | **4** | **3** | **5** |
| | 29 | Xways Forensics - Fundamentals | Level 3 - Competent | **3** | **3** | **5** |
| **Operating Systems - Technical** | 30 | Windows XP | Level 4 - Proficient | **4** | **3** | **5** |
| | 31 | Windows Vista | Level 4 - Proficient | **4** | **3** | **5** |
| | 32 | Windows 7 | Level 3 - Competent | **3** | **3** | **5** |
| | 33 | Linux | Level 2 - Beginner | **2** | **3** | **5** |
| | 34 | Mac OS | Level 2 - Beginner | **2** | **3** | **5** |
| **Lab Processes** | 35 | Quality Manual Processes | Level 4 - Proficient | **4** | **3** | **5** |
| | 36 | Operations Manual Processes | Level 4 - Proficient | **4** | **3** | **5** |
| | 37 | Health & Safety Manual Processes | Level 4 - Proficient | **4** | **3** | **5** |
| | 38 | Technical Manual Processes | Level 5 - Expert | **5** | **3** | **5** |
| | 39 | Audit and Peer Review Processes | Level 4 - Proficient | **4** | **3** | **5** |
| | 40 | Case Reports | Level 3 - Competent | **3** | **3** | **5** |
| | 41 | Case Presentation | Level 3 - Competent | **3** | **3** | **5** |
| **Soft Skills** | 42 | Analytical Thinking | Level 4 - Proficient | **4** | **3** | **5** |
| | 43 | Innovative Thinking | Level 4 - Proficient | **4** | **3** | **5** |
| | 44 | Teamwork & Cooperation | Level 3 - Competent | **3** | **3** | **5** |
| | 45 | Communication - Technical in Arabic (Written and Oral) | Level 3 - Competent | **3** | **3** | **5** |
| | 46 | Communication - Technical in English (Written and Oral) | Level 4 - Proficient | **4** | **3** | **5** |
| | 47 | Scripting | Level 2 - Beginner | **2** | **3** | **5** |
| | 48 | Documentation and Reporting | Level 4 - Proficient | **4** | **3** | **5** |
| | 49 | Research Skills | Level 4 - Proficient | **4** | **3** | **5** |
| | 50 | Problem-Solving Skills | Level 4 - Proficient | **4** | **3** | **5** |
| | **Individual total** | | | **183** | **150** | **250** |
| | **Individual average – Level 3 Competent** | | | **3.66** | | |

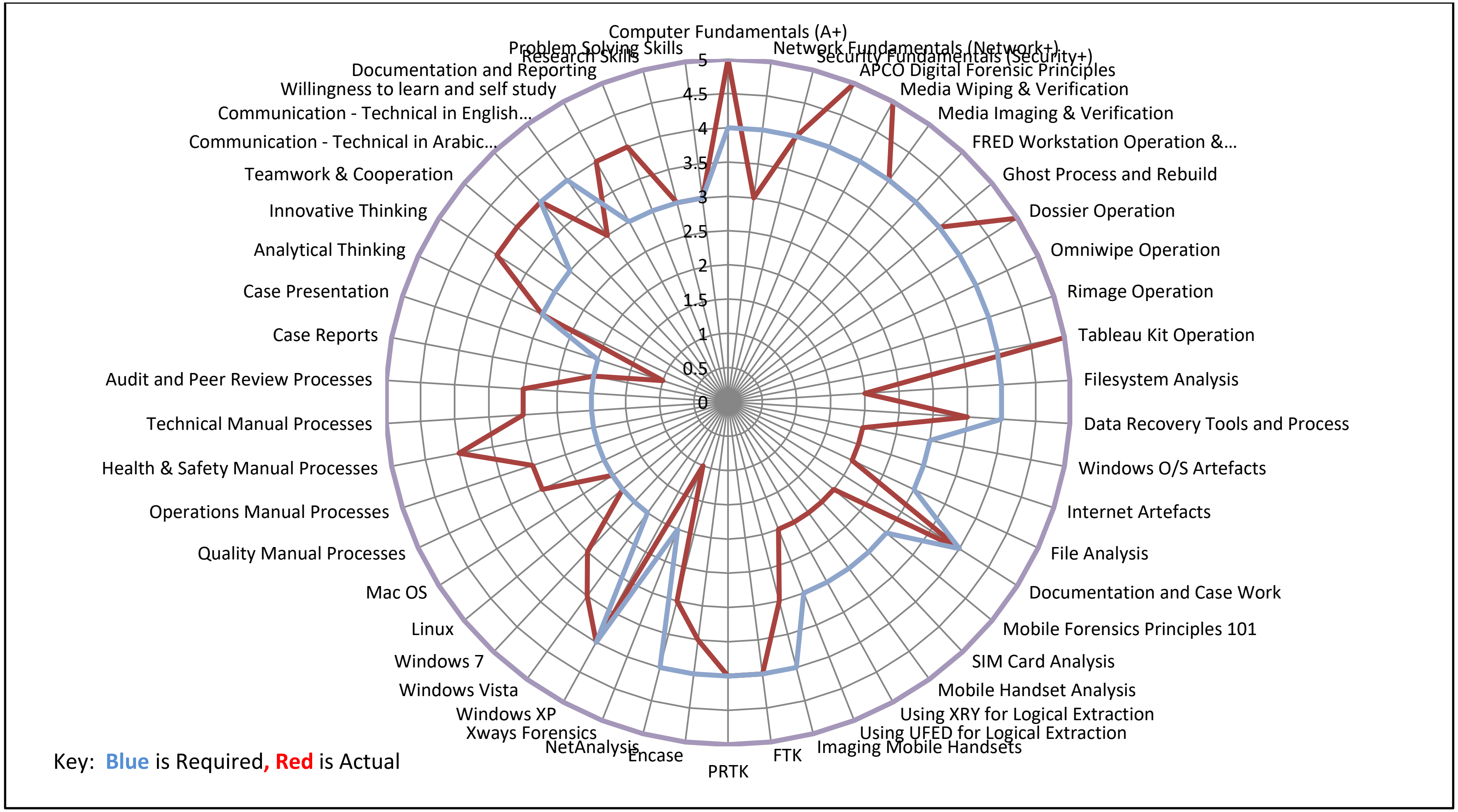


Figure 28: The actual versus required scores for the position of forensic engineer - lab #1

### 7.6.3 Forensic Examiner - Sample Summary Report & Comments Lab #1

Overall, the assessed individual (Forensic Examiner) exceeded the minimum skills requirements to perform their assigned duties within the lab in the majority of all areas. Areas where deficiencies were found could mostly be attributed to new projects for services not fully implemented and therefore not formally part of the lab's official services on offer. This would therefore explain why training in some of these areas had not yet been conducted.

The areas where deficiencies were found for this Examiner also applied to the majority (but not all of the other Forensic Examiners). Areas found to be lacking included:

- **Malware Analysis:**
  (Service currently delivered – Partial Deployment)
- **Mac OS & Linux Forensics:**
  (Service currently delivered – Partial Deployment)
- **Use of Flasher Boxes for Mobile Phone Extractions:**
  (Service currently delivered – Partial Deployment).

**Observation:** It was not possible to assess report writing during the assessment, as the majority of the reports for Lab #1 were restricted and confidential, and were not available for review during the assessment of Lab #1 – a fact that been overlooked during the creation of this tool and planning. Therefore, previous Proficiency test reports were used as the basis for report writing assessments.

### 7.6.4 People Domain Future Improvement

A key point noted was that personnel efficiency should be put into a context from a manager's perspective, to be able to assess an individual's P-CMM (theoretical) and actual Service Level Target compliance history for that individual measure (actual), factoring in the number of errors and non-conformances noted for that individual for the same period being assessed.

In theory, one could deduce a personal efficiency rating via the following basic formula:

*(P-CMM + SLT conformance) – Error Rate = Personnel Individual Efficiency Rating*

P-CMM would be calculated based on the P-CMM ratings on a scale of 1 to 5.

Service Level Target (SLT) Conformance would be calculated based on a scale of 1 to 5 based on past history of conformance with Service Level Targets where:

Service Level Target (SLT) Ratings would be:

- 5= Excellent – has met above 90% of all SLTs
- 4= Very Good – has met between 60 to 89% of all SLTs
- 3= Good – has met between 41% to 59% of all SLTs
- 2= Needs Improvement – has met between 21 to 40% of all SLTs
- 1= Poor – has met less than 20% of SLTs

Error or non-conformance rate would consider non-conformances, errors in work and documentation, and failure to complete required processes as prescribed by technical and operations processes.

These errors would be detected during technical and administrative ISO 17025 case audits and peer reviews, and would be tracked via a spreadsheet per examiner and rated as follows:

- 5= Excellent – Errors minor and seldom of high significance
- 4= Very Good – Errors minor and infrequent
- 3= Good – Generally few errors, and majority are of low significance
- 2= Needs Improvement – Frequent errors, of low to medium severity
- 1= Poor – Frequent errors of medium to high severity

This idea was generated from feedback and witnessing tests for Lab #1, but would require preparation on behalf of the lab to capture and record such data to make the assessment and calculations of ratings to be generated, as it relies heavily on historical data being available for review. This was noted as a possible improvement of the DF-C$^2$M$^2$ that would require additional research and exploration at a future stage of this research.

## 7.7 DF-C²M² ASSESSMENT OF THE PROCESS DOMAIN

The Process domain of the DF-C²M² and the related Assessment covers four specific areas, namely:

1. Policies and Procedures
2. Best Practices
3. Standards (National and International)
4. Regulatory and Legal Requirements.

### 7.7.1 Process Domain - Policies and Procedures Assessment

The key domains covered as part of the Processes assessments are:

- Quality Management System
- Health, Safety & Security
- Training
- Operations
- Technical
- Audit
- Validation of Tools & Methods (subset of Quality Management System)

#### 7.7.1.1 Assessment of Processes

Each area was assessed for completeness based on the DF-C²M² requirements and covered areas related to Quality Management, Operations, Health and Safety, Training, technical processes, Validation of Tools, Audits, and Best Practices.

#### 7.7.1.2 Assessor Comments

**Lab #1:** was found to have a solid, mature set of processes that have been fully implemented covering the design, review, and enforcement of these requirements.

**Lab #2:** was found to have a basic set of processes that had mostly been implemented. These processes fell short of the requirements of ISO 17025 and the DF-C²M².

The design and structure of Lab #1's organisational requirements exceed the baseline score of 3, but the overall organisational aspect is reduced by certain small elements that are well-documented within the lab's policies and procedures, but not as yet fully implemented, such as:

- Lack of quarterly quality committee meetings with customers.
- Lack of benchmarking results through external proficiency tests and inter-lab comparisons (for Mobile and Audio-Video).

However, the DF-C²M² Knowledge Base presented Lab #2 with an easy-to-implement roadmap for addressing these gaps and for fulfilling the requirements of both ISO 17025 and the DF-C²M² within a relatively short period of time, and with minimal cost of implementation – a clear demonstration of the DF-C²M²'s value proposition.

The summary score for the Process Domain Quality Management for each lab is presented in the table below:

| LAB | SCORE |
|---|---|
| Lab #1 | 3.24 out of 5 |
| Lab #2 | 1.8 of 5 |

Other Assessment tools worksheets for the Process area that follow such as Health & Safety, Training, Technical Processes, and Operations for Lab #1 are shown in Appendix E. The following findings were recorded as part of this stage of the Assessment process as illustrated via the Assessment Tool Quality Management Assessment Sheet in Table 42.

### Table 42: Process domain: quality management system – lab #1

| Category | Description | Score | | |
|---|---|---|---|---|
| | | Level | Rating | Required |
| **Q** | **Quality Management System** | | | |
| Q1 | Organisation has well-defined Digital Forensics Section Quality Policy endorsed by Executive Management. | Level 4 - Measured & Automated | **4** | **5** |
| Q2 | Organisation has well-defined Digital Forensics Section Vision & Mission Statement. | Level 4 - Measured & Automated | **4** | **5** |
| Q3 | Organisation has a set of well-defined of Internal and External Quality Objectives and KPIs. | Level 4 - Measured & Automated | **4** | **5** |
| Q4 | Organisation has Service Level Targets set for various typical categories of cases (or devices). | Level 2 - Partial Deployment | **2** | **5** |
| Q5 | Organisation has published its Service Level Targets to its customers and solicited their feedback on these targets. | Level 2 - Partial Deployment | **2** | **5** |
| Q6 | Organisation has an established Service Catalogue detailing services it is competent to offer (based on skills, tools, and procedures). | Level 3 – Full Deployment | **3** | **5** |
| Q7 | Service Catalogue is published to customers and revised/updated to maintain relevance at least annually. | Level 2 - Partial Deployment | **2** | **5** |
| Q8 | Organisational Quality, Vision, and Mission are clearly communicated to all personnel via regular refresher workshops and in internal Quality Management System documentation. | Level 3 – Full Deployment | **3** | **5** |
| Q9 | Organisation has defined roles related to Quality Manager within the team whose focus is improved service to customers, and compliance with standards, policies and best practices. | Level 4 - Measured & Automated | **4** | **5** |
| Q10 | Organisation meets customers at least quarterly as part of its Quality Committee to review customer satisfaction, complaints, improvements, and future services/changes. | Level 2 - Partial Deployment | **2** | **5** |
| Q11 | Quarterly reports issued to customers detailing cases received, cases completed, compliance with SLTs, number of devices examined, volume of data analysed, and number of complaints. | Level 4 - Measured & Automated | **4** | **5** |
| Q12 | Customers received a customer satisfaction form at completion of each case, where key areas related to service such as timeliness, communication, quality of report are rated. | Level 4 - Measured & Automated | **4** | **5** |
| Q13 | Customer satisfaction ratings are listed as a key department KPI and tracked on a case-by-case, quarterly, and annual basis. | Level 3 – Full Deployment | **3** | **5** |

|  |  |  |  |  |
|---|---|---|---|---|
| Q14 | Organisation has a well-defined Quality Manual detailing its Quality Management System, Organisation Structure, and KPIs. Personnel have been trained on the QMS. | Level 3 – Full Deployment | **3** | **5** |
| Q15 | Organisation has system for handling, approving, and tracking Corrective and Preventative Action Requests from customers and personnel. | Level 3 – Full Deployment | **3** | **5** |
| Q16 | Customers are free to submit complaints and personnel are required to record them within a Customer Satisfaction system. | Level 3 – Full Deployment | **3** | **5** |
| Q17 | Organisation has a designated document controller and system in place to ensure that obsolete documents, policies, and forms are removed from use once superseded. | Level 3 – Full Deployment | **3** | **5** |
| Q18 | Organisation has a system in place for Technical and Administrative Reviews of all cases and associated paperwork. Annual audits are conducted. | Level 3 – Full Deployment | **3** | **5** |
| Q19 | Organisation conducts an annual audit to check and measure overall compliance of all its related policies and procedures. | Level 3 – Full Deployment | **3** | **5** |
| Q20 | Organisation has well-defined Information Security and Confidentiality controls for all of its information, cases, and case reports. | Level 3 – Full Deployment | **3** | **5** |
| Q21 | Organisation has a code of conduct detailing personnel requirements, and in order to ensure impartiality in results, this is read and signed by all employees. | Level 3 – Full Deployment | **3** | **5** |
| Q22 | Organisation has well-defined roles and deputies defined and approved by Executive Management for roles of Lab Manager, Quality Manager, and Health & Safety Manager. | Level 3 – Full Deployment | **3** | **5** |
| Q23 | Personnel are free to escalate any issues affecting quality and results or due to non-compliance with policy by Lab Manager to executive management without fear of retribution, | Level 4 - Measured & Automated | **4** | **5** |
| Q24 | Any communications with customers related to a case are documented/recorded for each case and these logs may be subject to audit/review. | Level 3 – Full Deployment | **3** | **5** |
| Q25 | Reports produced by the department should be legally admissible in either a criminal or civil case, unless otherwise agreed in advance for a case by the Lab Manager & Customer. | Level 4 - Measured & Automated | **4** | **5** |
| Q26 | Lab Manager has a dotted-line reporting channel to Executive Management. | Level 2 – Partial Deployment | **2** | **5** |
| Q27 | Every Examination request received is documented and approved based on Organisation Policy requirements. No cases will be received without written request/warrant and approval from Lab Manager and referring customer's head of department. | Level 4 - Measured & Automated | **4** | **5** |
| Q28 | Organisation ensures that all equipment and tools used for examinations have been tested and pre-approved by the Lab Manager & Quality Manager prior to use on a case. | Level 3 – Full Deployment | **3** | **5** |

| | | | | |
|---|---|---|---|---|
| Q29 | Organisation has a process in place to handle approved deviations of policies and procedures. These would need to be approved by LM and the customer of the affected service request. | Level 3 – Full Deployment | **3** | **5** |
| Q30 | Organisation Policies and Procedures are reviewed at least annually, and changes made to any documentation occurs only following a peer review and approved Corrective Action. | Level 4 - Measured & Automated | **4** | **5** |
| Q31 | Organisation retains previous copies of all policies and procedures (including forms) for reference. These would be marked as Obsolete. | Level 3 – Full Deployment | **3** | **5** |
| Q32 | Organisational policies and procedures ensure continuity of Chain of Custody. | Level 3 – Full Deployment | **3** | **5** |
| Q33 | All organisational policies related to examination, evidence handling, and seizure conform to APCO principles for digital evidence handling at a minimum (and any legal requirements that may apply). | Level 4 - Measured & Automated | **4** | **5** |
| Q34 | Organisation has specially designated and separate areas for evidence handling, evidence storage, case files storage, imaging/extraction, examinations, and case previews. | Level 4 - Measured & Automated | **4** | **5** |
| Q35 | All lab personnel have clearly defined and authorised job descriptions describing their roles within the unit. | Level 4 - Measured & Automated | **4** | **5** |
| Q36 | Organisation has designated evidence custodian/gatekeeper responsible for logging cases, assigning case reference numbers, and evidence storage and retrieval. | Level 4 - Measured & Automated | **4** | **5** |
| Q37 | Organisation has well-defined data retention policy for all cases (derivative evidence) in compliance with legislative requirements. | Level 4 - Measured & Automated | **4** | **5** |
| Q38 | Organisation has well-defined data destruction policy and procedures for the case (derivative evidence) after the data retention period has expired. | Level 3 – Full Deployment | **3** | **5** |
| Q39 | Organisation has defined minimum training requirements per role per annum. | Level 4 - Measured & Automated | **4** | **5** |
| Q40 | Organisation has an approved operational budget for ongoing incidental expenses, storage media, and new tools and training (per annum). | Level 2 – Partial Deployment | **2** | **5** |
| Q41 | Organisation has well-defined policy regarding approved suppliers and use of sub-contractors (reviewed annually). | Level 4 - Measured & Automated | **4** | **5** |
| Q42 | Lab participates in benchmarking/lab proficiency tests annually to rate itself against other similar labs. | Level 2 – Partial Deployment | **2** | **5** |
| | **Total Score** | | **136** | **210** |
| | **Maturity Level Average** | **Level 3 - Full Deployment** | **3.24** | |

### 7.7.2 Process Domain - Health & Safety Assessment

Areas related to Health and Safety documentation and processes were assessed using the Assessment tool worksheet in Appendix E, and summary information is shown below:

**Lab #1** had strong Health and Safety policies catering to personnel equipment. Additionally, the policies address training, emergency management, and dealing with bio-hazards. Overall, areas related to Health and Safety are adequately addressed. However, opportunities for improvement exist based on the DF-C$^2$M$^2$ H&S assessment criteria items:

- HS4: Fire detection and suppression system (especially for evidence storage)
- HS7: Lab is monitored by a 24/7 Intruder/Panic System
- HS10: Lab has a disaster recovery plan that is implemented and tested at least annually.

The areas related to physical security, intruder detection, and automatic fire suppression systems should be enhanced.

**Lab #2** had good Health and Safety policies and procedures, but did not adequately address requirements related to bio-hazards as required by ISO 17025. The oversight would affect LAB #2's overall compliance ratings regarding overall process maturity and its ISO 17025 compliance requirements.

The inclusion of these results above is to illustrate the holistic use of the DF-C$^2$M for areas not just related to CMM and technical processes, but also as a tool to assist with assessing ISO 17025/ASCLD-LAB accreditation requirements.

### 7.7.3 Process Domain - Training Assessment

Areas related to Training assessment were reviewed using the Assessment tool worksheet in Appendix E, and summary information is shown below:

This stage of the assessment looked at policies governing training and the review of training records for lab personnel. The key areas assessed are best illustrated in the Assessment Tool Worksheet in Appendix E, and Lab #1 proved to provide the best example between the two labs to use as a point of reference and discussion. The design and structure of the Lab #1's training requirements exceed the baseline score of 3 – Fully Deployed. In contrast, the training requirements for Lab #2 mainly focused on technical tasks and did not cover Operational, Quality, and Health & Safety requirements for lab users (students). Lab #2 achieved a score of 2 – Partial Deployment.

### 7.7.4 Process Domain – Lab Operations Assessment

Areas related to Operations documentation and processes were assessed using the Assessment Tool Worksheet in Appendix E.

**Observations:** Essentially, both Lab #1 and Lab #2 had operational policies and procedures designed to suit their business and current accreditation requirements, which resulted in wide disparities between the two labs. Both sets of process documentation were suited for the intended purpose based on each lab's business requirements and accreditation status, but only Lab #1's Operational processes addressed the full requirements of the DF-C$^2$M$^2$ Process Domain – Operational requirements. This disparity would affect the creation of a general baseline for this area of assessment, but this was to be expected having realised this issue during the assessments. It was therefore decided that the long-term (future) solution to this and other disparities would be to classify labs based on their accreditation status and benchmark between labs of the same organisational type, e.g. accredited law enforcement vs another accredited law enforcement lab. Service categories not provided by a lab and their dependencies could be removed from the assessments, and Service Catalogue and training plans and not have major impact on the lab's overall conformance as the core requirements would still mostly be the same for all types of examinations conducted.

### 7.7.5 Process Domain – Technical Processes Assessment

The technical aspects of the Process domain were assessed for each lab, and the areas assessed are best illustrated as documented in the Assessment Tool Worksheet for Technical Processes in Appendix E.

Overall: Lab #1 demonstrated technically sound practical systems and policies in place that were in line with quality standards, accepted best practices, and legal requirements.

Lab #2, having not fulfilled all the requirements of the Service Catalogue, could only address items up to and including criterion Tec13.

### 7.7.6 Overall (Policies and Procedures) Assessment Summary – Lab #1

A final overall summary of the Process domain for each lab was created using the criteria from the Assessment Tool in Appendix E – Process Overall Worksheet.

Overall: Lab #1 has achieved good ratings, but the results were negatively affected by two key items, namely:

- O9: Clearly Defined Information Security Controls (documented, but several items require implementation of the controls not available), and
- O12: Quality Committee & Regular Stakeholder Reviews and Participation.

### 7.7.7 Process Domain – Best Practices Assessment

The key domains covered as part of the Best Practices assessments are General Best Practices, Technical Best Practices, and Quality Best Practices.

Other areas assessed under the process domain included Use of General, Technical Best Practices and Quality Best Practices. The Assessment Tool Worksheets for both sub-areas are included in Appendix E for reference.

## 7.8 TOOLS DOMAIN - ASSESSMENT OF VALIDATION PROCESSES FOR TOOLS

The Tools domain within the DF-C²M² addressed issues and challenges related to the requirements, risks, and costs associated with:

1. Use of non-validated tools and methods (from a legal and forensic science perspective).

2. Costs and time taken to test and validate newer versions of tools before authorised usage.

3. Impact associated with not using the latest, (possibly) more stable versions of tools due to lack of validation testing.

Experience has shown that a trade-off between maturity and stability of software releases exists in that in some instances as mobile forensics, the need for updated mobile forensic tools that support extraction and decoding of data for the newest handsets and applications is sometimes more important to an examination that the stability of the newer release of that mobile forensic application.

This trade would in most instances need to be assessed on a case by case basis by the lab management, and possibly involve the courts if the use of an untested/validate tool is to be used to produce or process evidence. Within computer forensics, the need to be using the lasts version of each tool is less critical and computer examiners would tend to prefer more stable rather than newer un-tested/validate versions of their tools

Within the DF-C²M², in addition to ensuring compliance with ISO 17025 and best practice forensic requirements for tool and method validation, this model includes validation of methods, verification of tools per use, and the inclusion of additional standards and best practices as ‘tools or methods’ that may be approved for use within a lab. The DF-C²M² Assessment of the Tools domain is done using the Assessment Tool Worksheets as follows in Table 43 to Table 45.

**Overall:** Lab #1 demonstrated strong enforcement of the Tools domain validation as well as verification of tools and methods, and of supplemental considerations such as the use of dual-tool verification as an additional means of verifying results.

Lab #2 followed the use of validated tools, however internal methods were found to have been validated as per ISO 17025 requirements. Additionally, tool verification prior to use and dual tool verification were not implemented as part of internal lab processes. As a non-ISO 17025 accredited lab, these findings were understandable, but affected the lab’s overall rating as per the DF-C$^2$M$^2$ requirements.

### Table 43: Tools domain - validation of tools assessment – Lab #1

| Category | Description | Score | | |
|---|---|---|---|---|
| | | Level | Rating | Required |
| **VT** | **Validation of Tools** | | | |
| VT1 | All primary tools used are validated. | Level 4 - Measured & Automated | 4 | 5 |
| VT2 | Lab has procedures to test and validate tools. | Level 4 - Measured & Automated | 4 | 5 |
| VT3 | Lab uses external validation results from established bodies such as NIST, etc. | Level 4 - Measured & Automated | 4 | 5 |
| VT4 | Lab has test data sets for tools testing. | Level 4 - Measured & Automated | 4 | 5 |
| VT5 | Lab has well-documented testing and validation processes. | Level 4 - Measured & Automated | 4 | 5 |
| VT6 | Qualified personnel conduct testing of tools. | Level 4 - Measured & Automated | 4 | 5 |
| VT7 | Validation test results are documented with data sets and retained indefinitely. | Level 4 - Measured & Automated | 4 | 5 |
| VT8 | Validation test results are shared with vendor (where issues arise). | Level 4 - Measured & Automated | 4 | 5 |
| VT9 | Validation test results are shared with other legally authorised peer labs. | Level 4 - Measured & Automated | 4 | 5 |
| VT10 | Personnel are trained on any new tools prior to implementation/authorisation. | Level 4 - Measured & Automated | 4 | 5 |
| VT11 | Personnel are competency tested on new tools prior to implementation. | Level 4 - Measured & Automated | 4 | 5 |
| VT12 | Workstation baseline builds are systematically updated with new tools. | Level 4 - Measured & Automated | 4 | 5 |
| VT13 | Technical SOPs and references are updated prior to implementation of new tools. | Level 4 - Measured & Automated | 4 | 5 |
| VT14 | Updates to tools are first reviewed and approved prior to implementation. | Level 4 - Measured & Automated | 4 | 5 |
| VT15 | All validation tests are technically reviewed to ensure that results are repeatable. | Level 4 - Measured & Automated | 4 | 5 |
| VT16 | Provision with QMS for deviation from using standard tools in exceptional cases. | Level 4 - Measured & Automated | 4 | 5 |
| **Total Score** | | | **64** | **80** |
| **Maturity Level Average** | | **Level 4 - Measured & Automated** | **4.00** | |

### Table 44: Tools domain – supplemental standards used (international and national)

| Category | Description | Score | | |
|---|---|---|---|---|
| | | Level | Rating | Required |
| **S** | **Standards (International and National)** | | | |
| S1 | Uses defined Standards for Digital Evidence Handling (Country-specific, if applicable). | Level 3 - Full Deployment | **3** | **5** |
| S2 | Uses defined International Standards for Digital Evidence Handling (ISO 27037). | Level 4 - Measured & Automated | **4** | **5** |
| S3 | Examiner Proficiency Testing (External). | Level 2 - Partial Deployment | **2** | **5** |
| S4 | Quality Management System (ISO 17025). | Level 4 - Measured & Automated | **4** | **5** |
| S5 | Quality Management System (ASCLD-LAB supplemental requirements). | Level 4 - Measured & Automated | **4** | **5** |
| S6 | Quality Management System (This Project's New Standard) | Level 3 - Full Deployment | **3** | **5** |
| S7 | Uses defined Standards for Information Security (International - ISO: 27001 or NERC CIP, etc.). | Level 2 - Partial Deployment | **2** | **5** |
| S8 | Uses defined Standards for Data Redaction. | Level 2 - Partial Deployment | **2** | **5** |
| S9 | Uses defined Standards for Media Wiping (e.g. DOD-5220.22M). | Level 4 - Measured & Automated | **4** | **5** |
| S10 | Uses defined Standards for Media Verification (e.g. MD-5 or SHA-1). | Level 4 - Measured & Automated | **4** | **5** |
| S11 | Uses defined Standards for Workstation/Tool Verification (e.g. SWGDE number). | Level 4 - Measured & Automated | **4** | **5** |
| S12 | Uses defined Standards for Wireless Signal Shielding for mobile phones. | Level 4 - Measured & Automated | **4** | **5** |
| S13 | Uses a well-defined Structured Training Plan (E.g. NIST's NICE Framework) | Level 3 - Full Deployment | **3** | **5** |
| | **Total Score** | | **43** | **65** |
| | **Maturity Level Average** | **Level 3 - Full Deployment** | **3.31** | |

### Table 45: Tools domain - validation of methods used

| Category | Description | Score | | |
|---|---|---|---|---|
| | | Level | Rating | Required |
| **VM** | **Validation of Methods** | | | |
| VM1 | All technical methods used are validated to ensure evidential integrity. | Level 4 - Measured & Automated | **4** | **5** |
| VM2 | Lab has procedures to test and validate new methods. | Level 4 - Measured & Automated | **4** | **5** |
| VM3 | Lab uses external validation results from established bodies such as NIST, etc. | Level 4 - Measured & Automated | **4** | **5** |
| VM4 | Lab has test data sets for new methods testing. | Level 4 - Measured & Automated | **4** | **5** |
| VM5 | Lab has well-documented testing and validation processes. | Level 4 - Measured & Automated | **4** | **5** |
| VM6 | Qualified personnel conduct design and testing of new methods. | Level 4 - Measured & Automated | **4** | **5** |
| VM7 | Validation test results are documented with data sets and retained indefinitely. | Level 4 - Measured & Automated | **4** | **5** |
| VM8 | Validation test results are shared with other legally authorised peer labs. | Level 4 - Measured & Automated | **4** | **5** |
| VM9 | Personnel are trained on any new methods prior to implementation/authorisation. | Level 4 - Measured & Automated | **4** | **5** |
| VM10 | Personnel are competency tested on new methods prior to implementation. | Level 4 - Measured & Automated | **4** | **5** |
| VM11 | Technical SOPs and references are updated prior to implementation of new methods. | Level 4 - Measured & Automated | **4** | **5** |
| VM12 | Updates to methods are first reviewed and approved prior to implementation. | Level 4 - Measured & Automated | **4** | **5** |
| VM13 | All validation tests are technically reviewed to ensure that results are repeatable and based on best practices/standards. | Level 4 - Measured & Automated | **4** | **5** |
| VM14 | Auditing process updated to cater to new methods. | Level 4 - Measured & Automated | **4** | **5** |
| VM15 | Provision with QMS for deviation from standard methods in exceptional cases. | Level 4 - Measured & Automated | **4** | **5** |
| | **Total Score** | | **60** | **75** |
| | **Maturity Level Average** | **Level 4 - Measured & Automated** | **4.00** | |

## 7.9 LABS ASSESSMENT SUMMARY AND RECOMMENDATIONS

### 7.9.1 Lab #1

Lab #1 provided an excellent, new, yet operationally mature site for this assessment and was found overall to meet at least 70% of ten new proposed DF-C$^2$M$^2$ requirements.

The lab has managed to achieve a good level of technical operation and quality management system maturity within a relatively short period of time. Further improvements are being implemented via process refinements, the introduction of automated pre-processing, and plans to implement a workflow-based case management system/Laboratory Information Management System (LIMS).

From an ISO 17025 perspective, the lab is a quality-driven, effective, and compliant lab, with minor areas for improvement. From a DF-C$^2$M$^2$ perspective, the lab was found to meet 70% of the new DF-C$^2$M$^2$ requirements, and could relatively easily and quickly achieve DF-C$^2$M$^2$ fully compliant status within a relatively short period of time, with no major changes to current operations.

Lab management should review the findings of this assessment with the view of addressing all issues raised, and plan to achieve a minimum overall rating per section of 4 out of 5. Having successfully implement ISO 17025, the lab's next challenge is to achieve improved operational efficiency, process, and personnel capability maturity, and to better utilise its existing processes, personnel, and tools to achieve higher-quality results with less effort, which can be achieved by implementing the DF-C$^2$M$^2$ requirements (supplemental and complementary to the current ISO requirements). The potential long-term benefits of compliance and participation with the DF-C$^2$M$^2$ may contribute towards allowing the lab to achieve:

A. A common Digital Forensic-specific baseline on which to plan, implement, and operate.

B. A common body of knowledge to leverage that is created by Digital Forensic lab members, for Digital Forensic labs.

C. Innovation and collaboration with peers via the DF-C$^2$M$^2$ knowledge sharing portal.

D. Reduced start-up and update costs for creating and writing new policies, procedures, and methods (via the use of the DF-C$^2$M$^2$ Knowledge Base).

E. Gains from reduced tools and method validation costs and time (via the DF-C$^2$M$^2$ shared validation tool testing platform).

F. Greater levels of technical, procedural, and operational excellence.

Feedback for select Lab #1 staff indicated a substantial interest in the DF-C$^2$M$^2$ and significant time savings and benefits to be derived from the DF-C$^2$M$^2$ framework, Body of Knowledge, and higher standards of review, assessment, and efficiency measurements compared with other stand-alone standards such as ISO 17025, etc.

From a design research perspective one could theorise that Lab #1 participants saw more value in the framework due to the experience in implementing lab processes and systems in accordance to ISO 17025, and having reached a certain level of maturity in their operations, they were perhaps more aware of the value that the model and its components could provide, but also this provided affirmation that the key design goal and resulting model were mostly in line with what labs such as Lab #1 needed to help address present gaps and operational issues.

Having more experience labs such as Lab #1 participate with a less established lab has provided a balance of view and opinions, and provided more realistic input as to how the model could be improved to suit both established and newly established labs. Being more experienced in lab operations and requirements; Lab #1 was better suited to also identify weaknesses within the model and approach and provide suggestions for improvements,

We recommend a review of these results with the lab, a discussion of findings, and a conversation to plan the next steps to benchmark this lab with other labs in the same region, same sector, and internationally.

### 7.9.2 Lab #2

Note: while CMM rating are generally given as integers, the DF-C²M² CMM ratings are given as averages across a given section evaluated and, as such may be displayed as non-integers e.g.: 3.5. In all instances the DF-C²M² CMM score given should be rounded off to the lowest value, therefore 2.5 would give an actual CMM rating of 2.

The overall score for Lab #2 was 79 out of 245, which indicates the average maturity level (across all sections) of (1.645) 1 out of 5, with the majority of the ratings per section being below 2. However, review and report parameters are above 2.0.

For the Process module, the majority of the categories scored more than 2.5, and the overall average maturity level is (3.15) 3 out of 5, which indicates full deployment in the policies and procedures. This is because the categories, such as technical, training, and tools, are very well-defined.

With respect to processes and best practice, the overall maturity level is partially deployed, with (2.25) 2 out of 5. General best practices scored highest because most of the tools used are industry standards, which are categorised and used for reporting purposes. Along with the software, hardware tools are used to acquire images, bit stream copiers, data wipers, and shadow copiers. Most of the tools are used and validated by creating images of different operating systems and analysing them using forensic software.

Few standards are used while performing the digital forensics during the coursework; most of the standards are taught during the course as theory but are not practiced, due to the cost and resource constraints.

Lab #2's overall People maturity level stands at level 2 and level 3. Staffing, work environment, performance, training, and compensation are very well-executed in the academic environment. Competency, workforce planning, career development, and participatory cultures all exist in the work environment, and most categories are defined and are effectively addressed.

Most of the tools used are industry standards. Therefore, the maturity level is partially deployed. Some of the procedures are person-dependent because of the theory and practical involvement in the course. Validation methods are mainly person-dependent; therefore, they are partially deployed. This module is mainly useful for commercial forensic labs for maintaining value, reputation, and standards.

The scores achieved by Lab #2 can be attributed to the facts previously stated, such as that the lab is only used as part of students' coursework and is not a fully operational digital forensic facility.

Based on the DF-C$^2$M$^2$ model, Lab #2 will require additional resources and expertise to expand its scope of services and investments in technologies. However, the DF-C$^2$M$^2$ has provided a framework to enable it to implement the various People, Processes, and Tools requirements to achieve capability maturity relatively quickly using the DF-C$^2$M$^2$ Knowledge Base and tools.

## 7.10 DF-C$^2$M$^2$ EVALUATION FEEDBACK

Upon completion of the DF-C$^2$M$^2$ workshops and assessments, practitioners from the two labs assessed were invited to participate in providing feedback and suggestions on the DF-C$^2$M$^2$ Model design via an evaluation form. The participant pool included lab managers from each assessed lab, and a select mix of practitioners from each lab. Four students were also solicited for feedback on elements of the model that they had seen during the workshops. The total number of workshop participants was 20.

The involvement of less experienced participants in the workshops and evaluations was seen by some of the more experienced practitioners as limitation due to their assumed limited experience, these individuals provided the most valuable insights on the usability aspects of the model, and how best to address their needs, and confirmation that the model had value to offer across a broad spectrum of practitioners and non-technical personnel. This broad cross-section of participants including managers provided insight and in some instances confirmation of the challenges affecting labs and how best to overcome them.

The DF-C$^2$M$^2$ evaluation form was used during interviews with Digital Forensic Practitioners, lab managers, academics, and trainees employed in law enforcement, government, and academic organisations. The evaluation form determined the demographic profile of each participant and information related to their current role, experience, education, geographic region, and whether they were employed by an ISO 17025/ASCLD-LAB accredited digital forensic laboratory.

The DF-C$^2$M$^2$ evaluation form consisted of 60 questions divided into 7 key areas:

1. General
2. DF-C$^2$M$^2$ Organisational Requirements
3. DF-C$^2$M$^2$ Service Catalogue
4. DF-C$^2$M$^2$ People Requirements
5. DF-C$^2$M$^2$ Process Requirements
6. DF-C$^2$M$^2$ Tools (and Methods) Requirements
7. Summary, Feedback, and Suitability of the DF-C$^2$M$^2$

For each question posed, the average or consensus rating is presented with further information regarding participant views shown in the results field for each question. The summary version of the evaluation form with consensus participant feedback as previously detailed in Appendix G.

Essentially, in all instances, the majority of participants agreed to the following key points taken from the evaluation form:

1. The DF-C$^2$M$^2$ was a valuable addition to existing ISO 17025 frameworks and systems.
2. The Model would enable their organisation to better measure and gauge their compliance status, and provided valuable insight into People, Processes, and Tools Maturity.
3. The Model provided a decision support system that would assist established and newly created labs to plan a route to achieving optimal performance and efficiency through the implementation and use of the DF-C$^2$M$^2$ tools and framework.
4. The DF-C$^2$M$^2$ filled a void within the present regime of standards and best practices with regards to capability maturity.
5. The DF-C$^2$M$^2$ could provide time and cost savings for labs implementing and maintaining ISO 17025 accreditation.
6. Of the existing models and frameworks that participants were aware of the majority had been too general or technically focussed, and none had provided a holistic or more comprehensive framework to plan, implement, and effectively manage People, Processes, and Tools elements of a digital forensic lab.
7. The Model is practically designed and structured around the three most important domains – People, Processes, and Tools (based on practitioner feedback).
8. The Service Catalogue provided a useful way, and structured way to plan, implement, and manage services within a lab.
9. The People Capability Maturity Model is sufficiently well-defined and is suited to the specialised field of digital forensics.

10. The concept of including People Capability Maturity within the Model would allow for organisations to plan for and achieve greater overall efficiency over an (as yet) undetermined period of time.
11. A standardised library of a vetted, regularly updated set of policies and procedures based on best practices and any relevant standards as part of the DF-C$^2$M$^2$ Body of Knowledge was cited as the most immediate benefit as suggested and by practitioners, therefore the reason for its inclusion within the planned roadmap.
12. The Six Steps Model provided a logical view and method for analysis of the digital forensic lab processes, and made sense to those who reviewed it.
13. Validations of tools and methods by testing and adoption of test results by DF-C$^2$M$^2$ participating labs will allow for better and faster testing of new tools and methods, and allow DF facilities to adopt newer tools and methods more quickly and at reduced cost (of testing).
14. The DF-C$^2$M$^2$ provides a sound framework and set of requirements for the People aspect of an internationally reputed DF facility.
15. The DF-C$^2$M$^2$ is implementable (with the DF-C$^2$M$^2$ Body of Knowledge) for the majority of organisations.
16. The DF-C$^2$M$^2$ will provide value and cost savings to many organisations.

The questions asked were top help determine issues as seen by the participants and to gain feedback on DF-C$^2$M$^2$. It was essential to determine if participants knew of other or similar model/frameworks at the time of the evaluations to determine if they saw value in the model, and if it was unique.

## 7.11 DF-C$^2$M$^2$ STRENGTHS AND WEAKNESSES

The journey in building and implementing the DF-C$^2$M$^2$ has proven to be challenging and encouraging. Most of the initial research assumptions regarding suitability and implementation of the DF-C$^2$M$^2$ proved to be accurate, and several unanticipated hurdles were encountered during the Assessment and Evaluation phases of this research that helped to provide insight on ways to improve the DF-C$^2$M$^2$, and in some ways, affirmation that the DF-C$^2$M$^2$ was effective, and evolving even during the Assessment phase.

The modular design and structure enabled on-the-fly adaptations and fine-tuning to help overcome certain issues, but also to refine the model based on findings in the real world through applied experience.

The DF-C$^2$M$^2$ proved to be a very effective method of assessing a lab, and using the findings of assessments to plot a path towards improvement and capability maturity appears to be an effective strategy; this will help to redress gaps within existing labs and standards via use of the DF-C$^2$M$^2$ Body of Knowledge components.

Some of the challenges faced that highlighted weaknesses within the DF-C$^2$M$^2$ included that fact that benchmarking of labs had to be done based on accreditation status, and non-accredited labs had no requirement to maintain rigorous documentation and records, thereby making certain aspects of the assessment difficult. The concept of applying the P-CMM to digital forensics has been proven via the DF-C$^2$M$^2$ to be possible, but real value would be derived from looking at the P-CMM and other aspects of an individual’s performance to determine the real or actual efficiency within a lab.

The DF-C$^2$M$^2$ was based on IS0 17025 accreditation requirements supplemented with additional best practices, tools, and prescriptive methods to assist labs in achieving and maintaining accreditation, but the DF-C$^2$M$^2$ would never become a standard as it presently stands, but perhaps form the framework and basis for ISO 17025 supplemental improvements, as sort of an ‘ISO 17025 ++’. Labs could still be assessed for DF-C$^2$M$^2$ compliance, but accreditation for DF-C$^2$M$^2$ adherence is not envisaged as an option in the near future.

The DF-C$^2$M$^2$ Body of Knowledge is voluminous, and this serves both as a strength and a weakness – a strength in that it represents a considerable volume of knowledge structured along the lines of People, Processes, and Tools, in a series of documents, forms, workflows, and checklists, but also a weakness in that improving the effectiveness, timeliness, and relevance of the DF-C$^2$M$^2$ as it presently stands can only being achieved through a collaborative community effort.

The DF-C$^2$M$^2$ assessment proved to be a learning experience and served to reinforce the original idea that the collective knowledge of the digital forensic community is what is better suited to assist organisations to finding solutions to legal, technical, and regulatory challenges, more than a standard body and committee ever could be.

Several assumptions about organisations and what to expect during the assessment were proven wrong, and the Assessment tool and Body of Knowledge had to be updated to adapt to the reality of the situations faced on the ground during the assessment. For example, the need to identify the underlying pre-requisite service for delivery of services had not been previously anticipated but was highlighted by Lab #1 participants as key aspect of service planning.

Likewise, it had been assumed that labs would have conducted some form of task analysis for each key role and identified the required skills and training required for personnel to perform various tasks, but this was found not to be the case, and a skill/task analysis was therefore performed using select participants from Lab #1 to create the task/skills/knowledge matrix, and restructure competency tests around these supporting knowledge and skills requirements.

The need to track performance utilisation of personnel per task was also highlighted as a key KPI in determining personnel capability maturity by participants and the P-CMM elements of the model were updated accordingly to reflect this.

The need to conduct competency testing of advanced tasks such as Analysis, Interpretation and Reporting of results was discovered to be lacking largely due to no requirements of effective means of doing as per the requirements of ISO 17025/ASCLD-LAB, and feedback and review of the existing ASCLD-LAB approved computer proficiency tests were found to be too basic, and the general consensus was that it should be used as a true measure of proficiency, as it covered what was considered by some participants to cover essentially evidence handling, tool verification, imaging and data recovery on a very small amount of data with low case complexity.

These findings helped revise various aspects and elements of the model and the assessment tool. Modularity of a framework that provides a degree of flexibility is important, as it enables scenarios not originally included within the framework to be incorporated, and enables updates and enhancements to be regularly included.

Overall, it is the view of the researcher and the consensus amongst participants that the DF-C$^2$M$^2$ is a viable and sustainable alternative to legacy standards, such as ISO 17025, that have proven to be ill-suited to digital forensics-specific sciences.

## 7.12 SUMMARY

This chapter highlights the key elements of the Digital Forensics – Comprehensive Capability Maturity Model (DF-C$^2$M$^2$). The DF-C$^2$M$^2$ Assessment tool has dual purposes in that it lists the DF-C$^2$M$^2$ requirements for each of the three core domains, and provides a way to measure compliance with these requirements.

The DF-C$^2$M$^2$ Assessment and Evaluation provide the validation of the DF-C$^2$M$^2$ proof of concept as a viable and better-suited means of digital forensic lab assessment and planning than is presently available.

The DF-C$^2$M$^2$ Body of Knowledge provides an insight into what was learned during this research, and key components of the Body of Knowledge have been highlighted in this summary. The Body of Knowledge is essentially a compendium created as part of this research documenting requirements, solutions, processes and tools that would be beneficial to mature and newly established digital forensic labs.

Work on the DF-C$^2$M$^2$ Body of Knowledge and on packaging the model and its deliverables into a simple-to-use and -follow system are still in progress. The samples shown here represent a sample of the Knowledge Base "Jump Start" Policies and Procedures. Forms are included but not shown here for brevity.

The DF-C$^2$M$^2$ Assessment tool forms an integral part of the DF-C$^2$M$^2$ Framework and Knowledge Base. The Assessment tool is included as part of this research for review and feedback.

# CHAPTER 8: CONCLUSION

## 8.0 INTRODUCTION

This chapter concludes by revisiting the research aims and objectives as outlined in Chapter 1, and by evaluating if theses aims and objectives were fully realised. This chapter will highlight the pros and cons of the proposed DF-C²M², lessons learnt, and any limitations discovered, as well as how these could be addressed. It will also discuss the viability of implementing the DF-C²M² on a national scale within a given country, and future directions for the DF-C²M².

### 8.1 DF-C²M² AIMS AND OBJECTIVES

The overall goal was to improve the quality and reliability of digital evidence, the quality of digital forensics investigations, and provide a means to determine Capability Maturity as stated in Chapter 1.

A secondary objective was to assess and determine whether existing digital forensic standards and models addressed the challenges often cited by practitioners.

To fulfil these objectives, the following research questions needed to be answered:

1. **Does the current system of accreditation of digital forensic labs fully address the core requirements of digital forensics as a scientific discipline, and are these accreditation requirements suitable to digital forensics?**

   Practitioner feedback through the participatory design stages proved invaluable in validating the model and its usefulness, but more importantly in helping to identify previously overlooked gaps and in determining how best to address them.

   During the workshops, assessments and during the evaluation provided the model was sustainable, but its level of success was dependent on the number of labs that chose to implement it, which in turn may be affected by the number of practitioners that have input into the model and its various elements moving forwards.

The model and its various components can assist labs in implementing and achieving CMM across its three organisational domains people, process and tool quiet effectively based on practitioner feedback.

Newer standards and best practices can easily be incorporated into the model providing a degree of flexibility and future-proofing or an organisation's strategy.

2. **What business drivers and challenges are increasingly affecting accredited labs in the goals to address the standard's requirements, whilst still being pressured with finding a most effective way to address the organisations' business drivers and constraints?**

   Lab assessments and practitioner feedback helped to identify and validate the perceived challenges, and the model provided a way to addressing some of these issues, and in helping to incorporate additional future requirements within the model and assessment tool to provide ongoing compliance assessments and measurements.

3. **Is capability maturity an overlooked means of achieving operational efficiency within digital forensics, and is it currently being addressed?**

   A review of two labs helped determine that capability maturity was a requirement, and that each lab was addressing the need differently, based on ad-hoc requirements or mandated performance management systems. Capability maturity and operational efficiency essentially and integrated, and achieving efficiency without maturity cannot be achieved in a sustainable and effective manner.

4. **By consensus, what would digital forensic practitioners and lab managers of new and established labs want to help them in order improve their efficiency, knowledge, and budget utilisation?**

   Ultimately the assessments and workshops provided insight that different levels of personnel required different things to assist them based on their role, and skills profiles. The model, being and its Body of Knowledge was able to address or provided solution for the major concerns and issues raised by practitioners, but this was heavily dependent on the completeness and breadth of the items included within the Body of Knowledge. Long-term success of the model would depend upon Body of Knowledge being up-to-date, relevant and useful.

5. **Are the current skills assessment, career development, and progression plans adequately defined within accredited labs? Are organisations able to effectively plan and measure their return on training investments?**

   The present training and career development regimes as determined through the surveys, and interviews remains very basic at best. The need for a unified or standardised recommended training and career progression plan for various roles found within a typical digital forensic laboratory are critical, and P-CMM can only be achieved maximised through sound training, skills assessments and career development plans. The model via the assessments tool and body of knowledge help in part to address these issues and provide a possible way forward for the industry as a whole.

6. **Would better planning for forensic services and incident response allow for faster gains for organisations if they had the foresight and knowledge of the main services, their prerequisite requirements? Would this enable labs not currently accredited to be able to gain accreditation sooner and at a lower cost?**

   While the service catalogue was found to be useful during workshops and the use of the catalogue as a planning tool to help identify service prerequisites, required skills, tools and processes – few other than some senior examiners and managers appreciated the usefulness of the catalogues as a planning tool especially its value when combined with the assessment tool, and using the Body of Knowledge to remediate shortcomings.

   The Body of Knowledge proved key to assist organisational in augmenting their current processes and in helping organisations implement ISO 17025 compliant digital forensics processes.

7. **Can this new alternative model cater to both existing and newly founded digital forensics labs?**

   It was determined via the workshops and assessments that the model can cater for new and existing digital forensic lab requirements, but the researcher’s decision to hinge the framework on ISO 17025 requirements, mean that the labs would need to implement the core if not all off the requirements of ISO 17025 regardless of whether they intend to be accredited to fully benefit from the model.

## 8.2 MODULARITY & DESIGN GOALS

Creating a framework that would provide information, know-how, and processes in a timely, relevant, extensible, and modular structure were key design goals that received positive feedback during the participant evaluation of the DF-C$^2$M$^2$.

The DF-C$^2$M$^2$ was designed to address the cited challenges by creating a modular management decision support framework to enable labs to better manage and achieve their objectives through a system of assessments and planning tools all geared towards measuring compliance and capability maturity across multiple domains.

The DF-C$^2$M$^2$ was designed to equip existing and new labs with an operational framework and Body of Knowledge to enable them to quickly align themselves with existing standards and best practices in an easy and cost-effective manner.

## 8.3 DF-C²M² EVALUATION

This research provided a great deal of insight into the actual challenges and issues that digital forensic labs face when trying to manage pressing regulatory, accreditation, and productivity challenges.

This research addressed the initial research objectives and aim, and demonstrated that:

- The current system of accreditation of digital forensic labs provide the framework upon which quality management controls can be implemented, but more is required to address the requirements of digital forensics as a scientific discipline and that these accreditation requirements. Whilst accreditation standards have provided useful in helping to bring a level of credibility to digital forensic laboratories, these standards do not address the current challenges from a holistic and bespoke perspective and there is a need to supplement the standards with a model that will address capability maturity issues and concerns across the people, process and Tools organisational domains.

- The present accreditation regimen has been demonstrated through practitioner feedback as being costly and time consuming to develop and maintain internal policies and processes compliant with the ISO 17025/ASCLD-LAB requirements, and the model can assist in helping to reduce the associated costs via the targeted assessment tool and body of knowledge.

- It was discovered that the present system of accreditation for digital forensic labs does not directly contribute towards helping an organisation to achieve operational efficiency and to measure capability maturity, although this system did help organisations to improve lab processes via the cornerstones of quality management – the Shewhart Cycle (Plan, Do, Check, Act) and the Corrective Action process (Deming, 2000).

- The consensus view from practitioners was that the current standard and system for accreditation of digital forensic laboratories does not provide labs with an effective way to pool collective knowledge and best practices from participating labs and practitioners.

- The gaps within the present regime of international standards related to digital forensics labs were numerous, as cited in Chapter 3. Although recently released standards such as ISO 27041 and ISO 27042 help to address some issues, they are still primary geared towards internal information security incident response teams, and do not attempt to integrate with ISO 17025; rather, they create a duplication of requirements when comparing requirements such as validation and verification of tools.  Additionally, they failed to address the People, Processes, and Tools requirements of an organisation in a systematic, holistic, and integrated manner.

- Proficiency testing – whilst mandated as part of ISO 17025 accreditation for personnel, this was historically found to be lacking, with accredited proficiency testing for Mobile Forensics having only been introduced in 2015 (Collaborative Testing Services, 2015).

- Additionally, practitioner feedback indicated that existing digital forensic standards and models were often either too general, or too technical and specific, and did not provide a holistic scheme to address the majority of the most critical and significant challenges faced by digital forensic laboratories within the People, Processes, and Tools domains holistically. The results of the participant's evaluation of the model are shown in Appendix G.

### 8.3.1 DF-C²M² Key Findings

Through the series of detailed interviews, surveys, digital forensic model reviews, and lab assessments as part of this research, it was determined that:

1. The current state of play regarding digital forensics standards and the implementation issues related to implementing these standards were affected by primarily a lack of attention to three inter-dependent domains, People, Processes, and Tools.
2. Of the few existing models and frameworks that attempted to address one of the three key organisational domains, they often neglected the inter-relationship and dependencies with the other domains.
3. ISO 17025 was found to be ill-suited specifically to digital forensics, and that attempts to translate some of the requirements into practical guidance in digital forensics was cumbersome and very much subject to interpretation by assessors.
4. The current digital forensic laboratory standards, as they are sometimes known, were in fact nothing more than a collection of subject-specific (technical) best practices, and an ill-suited legacy standard for testing laboratories (ISO 17025) adopted to provide a basic premise upon which digital forensic labs could be assessed and accredited, as dictated by various regulatory authorities in different countries.
5. The cost of designing processes and procedures to be compliant with existing standards was often seen as an unavoidable expense rather than an investment, and the ongoing administrative overhead of implementing and maintaining compliance with standards was seen as a major obstacle that hindered productivity.
6. The present regime of tool validation had created major challenges with organisations faced with the decision to either use older, validated tools (at the risk of missing potential evidence), or investing heavily with time and resources to test each and every version of the wide range of tools commonly used.
7. Several deficiencies within the current training and career development regimes that extended to digital forensics competency and proficiency testing were discovered within the labs assessed. It is feasible that these same or similar deficiencies would be found in other comparable labs due to the lack of a

formally regimented and structured digital forensics training and career development path within the industry as a whole.

8. When evaluating the ranges of services offered by various digital forensic laboratories, there was little tangible evidence of any significant planning of the scope of services and the pre-requisites specifically as they apply to People, Processes, and Tools.
9. Services were often planned and implemented in an ad hoc manner to address the immediate requirement, with required documentation being drafted to provide the most basic set of instructions or guidance in order to help meet the ISO 17025 requirements.
10. Within organisations, the lack of formal, published service catalogues may result in customers understanding very little about the features and limitations of any given service. Additionally, the implementation of service levels based on the service type was an idea not yet implemented amongst practitioners and labs assessed, who seemed divided about how best to determine service levels based on the type of device, volume of data to be examined, and case complexity. Many agreed that service levels were important, but the group could not find a consensus of what the service level targets should be.
11. Regulators seemed not to fully appreciate the extent of the challenges faced by digital forensic labs in maintaining quality and efficiency, and meeting statutory and regulatory requirements.
12. Most regulators had simply stipulated compliance with ISO 17025 as being required, without recognising the challenges and complexities that labs faced, and with little acknowledgement of its deficiencies and how to remediate them.
13. In reality, it was discovered that true ISO 17025/ASCLD-LAB compliance could only really be applied to Computer and Digital Video forensic requirements, not to Mobile Forensics due to a lack of the required approved external proficiency tests for Mobile Forensics not being available until recently (March 2015) (Collaborative Testing Services, 2015).
14. The implication of this was that digital forensic laboratories providing computer and mobile forensics services were technically only fully accredited for Computer and not Mobile Forensics, as there were no ISO 17043 approved Mobile Forensic test providers until very recently in 2015.

15. Additionally, Table 46 shows the various Digital Forensic-related standards including newly released standards addressed within DF-$C^2M^2$.
16. The DF-$C^2M^2$ addresses each of the technical and non-technical challenges discussed in Chapter 2 by providing a means through which labs can assess how well they are addressing their compliance, accreditation and capability maturity challenges, including People, Process, and Tool-related issues that could affect or impede an organisation's capability maturity as it related to Digital Forensics. Additional challenges identified during this research have been added to the list of Challenges (see Table 47).

**Table 46: Mapping digital forensic standards requirements to the DF-$C^2M^2$**

| Digital Forensic Related Standards | DF-$C^2M^2$ | | Addressed within DF-$C^2M^2$ across all 3 domains |
|---|---|---|---|
| | ISO Related Standards | | |
| | 1 | ISO 17025 Requirements | ✓ |
| | 2 | ASCLD/LAB Requirements | ✓ |
| | 3 | ISO 27037 Requirements | ✓ |
| | 4 | ISO 27041 Requirements | ✓ |
| | 5 | ISO 27042 Requirements | ✓ |

### Table 47: Digital forensic challenges

| | DF-C$^2$M$^2$ Category | | Organisational | Process | People | Tools & Methods | Addressed within |
|---|---|---|---|---|---|---|---|
| | Challenge | | (Legal & Regulatory) | (Standards & Best Practices) | (Training & Certification) | (Technological) | DF-C$^2$M$^2$ across all 3 Domains |
| Digital Forensic Challenges | 1 | Technology changes/diversity | | | | ✓✓✓ | ✓ |
| | 2 | Video and rich media (Multimedia) | | ✓ | | ✓ | ✓ |
| | 3 | Encryption | | ✓ | | ✓✓ | ✓ |
| | 4 | Wireless | | ✓ | | ✓ | ✓ |
| | 5 | Anti-forensics | | ✓ | | ✓✓ | ✓ |
| | 6 | Virtualisation | | ✓ | | ✓ | ✓ |
| | 7 | Live response | | ✓ | | ✓ | ✓ |
| | 8 | Distributed evidence | | ✓ | | ✓ | ✓ |
| | 9 | Usability & visualisation | | | | ✓ | ✓ |
| | 10 | Volume of evidence (data) | | | | ✓✓✓ | ✓ |
| | 11 | Education & certification | ✓✓ | ✓✓ | ✓✓ | ✓✓ | ✓ |
| | 12 | Embedded systems | | | | ✓ | ✓ |
| | 13 | Forensic readiness | ✓✓ | ✓✓ | ✓✓ | ✓✓ | ✓ |
| | 14 | Monitoring the internet (Intelligence) | ✓ | ✓ | ✓ | ✓ | ✓ |
| | 15 | Tools (development, testing) | ✓ | ✓ | | ✓ | ✓ |
| | 16 | Networked & online evidence (cloud data) | | ✓ | ✓ | ✓ | ✓ |
| | 17 | Adapting to shifts in law/regulation | ✓ | ✓ | | | ✓ |
| | 18 | Developing specific standards | ✓✓ | ✓✓ | ✓✓ | ✓✓ | ✓ |
| | 19 | Capability or Process Maturity (to some degree) | ✓ | ✓ | ✓ | | ✓ |
| | 20 | Social networking platforms/apps | | | | | ✓ |
| | 21 | Need for a common knowledge base of processes, methods, and workflows | | | | | ✓ |
| | 22 | Tool to plan & measure services & capabilities | | | | | ✓ |
| | 23 | Service Catalog that identifies services & underlying prerequisites (People, Processes, Tools) | | | | | ✓ |

**Legend:** ✓ - represents count for number of times item was raised as a challenge during the review of previous surveys of frameworks and models.

Through the various interviews, model reviews, and assessments, several valuable results were obtained during the workshops including:

1. The Model required a tool that enabled assessment and measurement across all areas of the proposed model from ISO 17025 compliance through to workflow and method validation, and competency and skills matrices. The result is that the existing tool was updated to include and encompass these elements.
2. The overall goals and objectives of the model were achieved based on the outcomes of the lab assessments, peer reviews, and planning roadmap produced at the end of the assessment exercise.
3. The design goals were found to be realistic, and the challenges faced by labs were expanded upon slightly to consider various unique aspects not previously factored into the assessment and decision-making support tool.
4. The model has proven to be useful, and via minor enhancement of the tool’s interface, is easier to use for assessments, but also in the future for benchmarking of labs against the criteria.
5. The assessment criteria for all aspects covered by the model were found to adequately address all necessary planning, implementing, and management tasks.
6. There is a definite need for the proposed model within both accredited and non-accredited digital forensic labs as a gap analysis and improvement planning tool.

Capability Maturity is a major concern for many practitioners and labs, although some had not defined the issues faced or goals to which they aspired within the Capability Maturity terminology; however, essentially improved capacity, efficiency, and capability were all key goals of many of those interviewed.

### 8.3.2 Limitations and Lessons Learnt

#### 8.3.2.1 Limitations of Scope

Based on the evaluation and feedback results of the DF-C²M², key issues that could have allowed for a more comprehensive review and feedback include:

1. Having access to more potential labs to conduct the DF-C²M² assessments and review workshops would have provided a much broader set of feedback and areas for improvement. Likewise, this would have contributed to creating a baseline upon which other labs could be more accurately benchmarked for compliance and capability maturity.

2. Addressing business issues such as providing tangible proof of increased employee productivity via implementation of the DF-C²M² were recognised as key additions to the DF-C²M², in order to substantiate the theory of business savings and cost benefits, rather than relying purely of the perceived cost savings. This would need to be included within the DF-C²M² at a later stage to help quantify the actual business savings.

3. Feedback from more ISO 17025/ASCLD-LAB assessors on the DF-C²M² and the use and suitability of the DF-C²M² Assessment tool would have been beneficial to providing additional insight into issues faced by assessors and how the DF-C²M² Body of Knowledge and tools could be further improved.

4. Broader peer review and feedback on the DF-C²M² from the broader digital forensic community at large would undoubtedly provide greater value and insight in the future.

5. Consumers of digital forensic lab products (reports and findings) were not included within the scope of this research, although customer feedback and customers' satisfaction requirements were factored into the model, and included as elements within the Body of knowledge.

### 8.3.2.2 Other limitations discovered during this research include:

1. The final release of ISO 27041, and ISO 27042 in the latter half of 2015 were not sufficiently covered in the design of the model, and the assessment tool at the time of the evaluations and lab assessments were conducted. Although an outline of what the standards would include was known, the final standards and their requirements were not, and therefore analysis, interpretation and reporting of results are key areas that were not sufficiently covered in the assessments, and the body of Knowledge.

   Following the release of these new, related standards, discussion with both participated labs indicated that they were looking at implementing these standards, but no time frame had been set and they would be keen to see how DF-C$^2$M$^2$ would enable them to implement and asses these requirements in the future.

2. The assessments performed were almost akin to detailed audits, and although Labs #1 and #2 were very accommodating, the need to have independent auditors capable of performing DF-C$^2$M$^2$ assessments would be key to the long-term viability of the assessments. The possibility of using the DF-C$^2$M$^2$ assessment tool to supplement existing ISO 17025/ASCLD-LAB assessors in their assessment of digital forensics labs, was explored briefly in discussion with an ISO 17025 auditor, but broader acceptance of such an approach would be required for organisations to be independently assessed by trusted third parties. For now, the assessment tool can be used at least by internal auditors, assessors and managers to plan future services, assess needs and measure ISO 17025/ASCLD-LAB compliance.

3. The length of time to deliver the workshops and to perform the assessments (including witnessing of tests) was under-estimated, but asking the participants for additional time to complete the assessments in more detail may not have been achievable. Lab #1 was able to allow for more time for certain participants to participate. Providing the assessment tool for labs to perform self-assessment is one solution to addressing this, but a full assessment with a detailed audit report would require at least four to days at

present involving one assessor and at least 10 participants for the participating lab.

4. The model perhaps could have been better refined, by not including Cybercrime Analysis within the scope and perhaps utilising that time to incorporate the requirements of ISO 27041 and ISO 27042 within the scope to address the Analysis, Interpretation and Reporting of digital evidence results. By reducing the scope and focussing purely on digital forensic related requirements, the model would have been more comprehensive, and specific. However, it should also be noted that these ISO standards were released in later in 2015, by which time the bulk of the research, and creation of the assessment tool, and body of knowledge had mostly already been completed. At the same time, it should also be noted that Cybercrime was included to demonstrate modularity of the model and how CMM could also apply to People, process and Tools for Cybercrime units.

5. The use of the assessment tool required a degree of familiarity with the exiting lab operations, policies and procedures, and with ISO 17025 as the basis for Lab #1's policies and procedures, this process was relatively straightforward to achieve, however, with Lab #2, their existing policies and procedures were compliant with some aspects of ISO 17025, but they also had a vast number of processes informally documented and evaluating these prior to the assessments was essential, but not previously anticipated at the start of the assessment.

6. Certain assumption regarding business needs and challenges prior to commencing the research were found to be correct, but how best to address these in an easier, and more systematic way was often debated during some of the workshops. A broader community input and consensus on key elements of the model and assessment method is required for the model to gain a more universal acceptance.

7. Creating benchmarks for labs may seem like the way forward as far as CMM and ISO 17025 compliance is concerned and many participants expressed an interest in seeing how they or their labs would fair be compared to others. However, the practicality in view of privacy concerns that other labs may have in future to enable the success of such a benchmarking system is as yet unknown, and only possible through broader industry participation and acceptance.

8. Workflows created for technical processes and procedure as learning aids and part of the body of knowledge tools domain, included names of sample products, whereas they should have made non-product specific. These changes can be implemented relatively quickly without affecting the overall body of knowledge.

### 8.3.2 Areas for Improvement

It was assumed that providing a way of incorporating the P-CMM into processes, staff assessments, and lab evaluations would provide management with valuable insight into how efficient their personnel were. However, as pointed out during the lab assessments, the P-CMM is seen as a purely theoretical measure for personnel efficiency.

Real efficiency would need to factor in the P-CMM, conformance with Service Level Targets, and the Error rating per individual to determine a more concise and valuable means to measure personnel efficiency. Thus, a new proposed, and yet untested, formal structure was created to help resolve this oversight and address compelling business performance and efficiency requirements.

A reconsideration of the grouping of labs of similar accreditation status is required in order to overcome discrepancies encountered during the labs' assessments, and to enable benchmarking between comparable laboratories in the future.

The original time estimates for assessments were grossly underestimated, in view of the extensive scope of the assessment, based on the DF-C$^2$M$^2$ assessment tool and Body of Knowledge.

Broader community participation and feedback will be critical to help refine both the design and elements of the DF-C$^2$M$^2$, and to assist with the DF-C$^2$M$^2$ becoming a de facto organisational digital forensics best practice in the absence of any standardised offerings or frameworks.

## 8.4 DF-C²M² FUTURE DIRECTIONS

The DF-C²M² was designed and implemented using a consultative research approach, and intends to address the numerous issues and challenges faced by digital forensic laboratories and practitioners. The modular design goals enable additional standards or regulatory requirements to be easily incorporated into the model as well as the CMM and P-CMM processes and criteria.

Initial feedback from experienced practitioners and those relatively new to the profession alike indicate acceptance of the model, its framework, and approach. As proof of concept, an existing digital forensic lab has agreed in principle to implement key elements of the model as a means of augmenting their current systems.

The model and its original goals have been validated by a cross-section of practitioners, and applicability of the model on a broader scale is both practical and achievable, and will provide value to labs choosing to adopt the model to augment their current processes, and new labs wishing to establish processes with CMM included as a key business objective.

This research and its outputs provide a solid foundation to assist could potentially be used by ISO 17025/ASCLD-LAB digital forensics assessors and auditors with tool to augment their assessments and to enable auditee labs to remediate possible non-compliance issues via Body of Knowledge.  Using the core framework, workflows and controls to create a Digital Forensics' specific laboratory case management/laboratory information management system has been suggested, and may be a possible area of future work.

Incorporation of the requirements of ISO 27041 and ISO 27042 related to the examination, analysis, interpreting and reporting of digital evidence into both the Body of Knowledge and the Assessment tool, are the foremost priorities to extend the value of the model, and to address areas that were previously not covered in as much detail.

While initial feedback of the model has been extremely positive, what remains to be seen is the broader digital forensics community's acceptance of the model, its Knowledge Base, and its assessment and planning tools. Additionally, how to implement the model on a national scale within a given country, whilst feasible, requires additional work, including planning and promoting the model with all law enforcement and judiciary stakeholders. It is anticipated that lessons on how best to package, deliver, and measure the success of the model in various law enforcement laboratories will help to further refine the model and its various key components. Releasing the model, assessment tool and body of knowledge under an open-source/gnu license will lead to greater feedback on improvements and acceptance of the model as a viable solution for digital forensic labs as part of the business process improvement and capability maturity goals and initiative.

The initial plan for nationwide implementation of the model will begin following the complete assessment of two labs, followed by full implementation assistance and a follow-up assessment six months later. Key Performance Indicators (KPIs) taken before and after the implementation period will be gathered and used as part of the final business case proposal to the relevant ministers responsible for law enforcement and the judiciary.

A planned series of workshops using data gathered from the two labs will be conducted for other interested law enforcement digital forensic laboratories.

Training for all lab management and personnel will be delivered over a period of six months with consultation visits from several invited ISO 17025/ASCLD-LAB accreditors. The final assessment and analysis of the KPIs previously identified, as well as associated cost savings and improved productivity reports, will then be published shortly thereafter.

Two compelling business arguments drafted as part of this national implementation plan are that:

1. With one ISO 17025 accredited law enforcement lab, disparity may exist in cases where evidence processed by several labs within a given jurisdiction or country are submitted as part of the same case. The need for a uniform standard of evidence processing across all law enforcement labs therefore becomes vital to ensuring the quality and integrity of all cases, including cross-jurisdictional cases.

2. The various benefits and cost savings of achieving levels of maturity and accreditation by implementing the DF-C$^2$M$^2$ as a national model are accessible

to both law enforcement and non-law enforcement digital forensic labs as a national best practise.

**The next steps would include:**

1. To pursue the goal of applying the DF-C$^2$M$^2$ as a best practice for law enforcement digital forensic laboratories using the plan briefly outlined above.
2. To submit the DF-C$^2$M$^2$ to the broader digital forensic and associated community via the DF-C$^2$M$^2$ community portal for review and implementation, and to enlist member labs that will be willing to contribute towards the ongoing maintenance and development of the DF-C$^2$M$^2$, its tools, and its Knowledge Base, and to launch the DF-C$^2$M$^2$ community tool and methods testing validation results.
3. Submitting the DF-C$^2$M$^2$ as a technical best practice under the auspices of an existing standards body is an option that will be reviewed after broader community exposure and feedback regarding the DF-C$^2$M$^2$.
4. Following the implementation of the above, a review and re-evaluation of the DF-C$^2$M$^2$ and its contribution towards an improved set of tools for managing and establishing ISO 17025 via 'before and after' assessments of digital forensic labs, would help to identify the overall success and impact that the DF-C$^2$M$^2$ has had towards addressing digital forensic organisational challenges and in enabling capability maturity as a key goal and metric within digital forensic lab objectives, KPIs, and long-term business drivers.

The long-term vision for the DF-C$^2$M$^2$ would be to create an open, contributory community of digital forensic practitioners, labs, and interested parties (as a non-profit organisation). The goal of the DF-C$^2$M$^2$ community would be to help define the new standards and best practices for Digital Forensics, and provide participating members with a current and up-to-date, accreditation-centric, peer-reviewed Body of Knowledge to assist them in implementing these elements and thereby enable them to achieve greater efficiency and proficiency in the areas of Digital Forensics, and provide a common set of bespoke criteria that digital laboratories can be assessed and benchmarked against globally.

The DF-C$^2$M$^2$ community would allow laboratories to address the existing challenges and business concerns, and help further their development and ongoing cost of maintaining and managing ISO 17025/ASCLD-LAB compliant procedures and requirements in a timely and cost-effective manner.

Proposed long-term financing for the DF-C$^2$M$^2$ could be provided through partnerships, subscriptions, certifications, licensing, seminars, and possibly private research endowments. Membership and voting for adoption and changes to the DF-C$^2$M$^2$ Body of Knowledge, updates, and appointment of assessors will be done by all participating member organisations and individuals. Key stakeholders will be appointed from existing standards and accreditations bodies, leading universities, law enforcement laboratories, and digital forensic practitioners.

An example of the DF-C$^2$M$^2$ Body of Knowledge Best Practices includes simplified process workflows with added explanations. The workflows form parts of the DF-C$^2$M$^2$ SOPs, each with an accompanying set of narrative instructions (Step by Steps), related forms, checklists, and audit controls/guidelines. These SOPs will also form the basis of on-the-job training and mentoring requirements for participating labs, and can be adapted as required by any of these labs as long as key steps (deemed critical) are not omitted. The DF-C$^2$M$^2$ will issue guidelines on which steps are or are not critical in each of these SOPs. These workflows and narratives make up key components of the model.

For initial industry acceptance, the requirements of ISO 17025 and ASCLD-LAB (with all ASCLD-LAB and DF-C$^2$M$^2$ supplemental controls) will form the foundation that the DF-C$^2$M$^2$ framework will rely upon. The DF-C$^2$M$^2$ Body of Knowledge will form a key element of the DF-C$^2$M$^2$, and provide the overall content for the DF-C$^2$M$^2$ framework.

It is possible that the DF-C$^2$M$^2$ will evolve into a more adaptable, digital forensics-specific international standard compatible with ISO 17025 and ASCLD-LAB current accreditation requirements for digital forensics laboratories that can be applied to three levels of digital forensics labs: commercial, non-law enforcement, and law enforcement. Each category of accreditation will have the same overall set of requirements, but with some minor differences based on the nature of digital forensic examinations conducted (determined by organisation type). For example, organisations that are involved in the seizure and collection of digital evidence from crime scenes would need to include the DF-C$^2$M$^2$ supplemental requirements based on ISO 27037. Commercial firms are defined as organisations that provide paid digital forensic services to other external organisations or entities.

## 8.5 DF-C²M² REFLECTIONS AND PROPOSAL

Digital Forensics Capability Maturity is now a necessary, overlooked aspect of Digital Forensics Quality Management that has been identified as an essential business and quality assurance requirement.

The Digital Forensics – Comprehensive Capability Maturity Model (DF-C²M²) was born out of the findings of this research, and the scientific gap that exists in the current digital forensics standards, best practices, frameworks, and models.

This research demonstrated a novel and yet holistic approach to addressing the challenges faced by digital forensic organisations via the design and implementation of a comprehensive, modular and readily extensible framework –the DF-C²M².

The DF-C²M² design goal was to create a reliable, readily accessible extensible/modular framework that would enable an organisation (regardless of its present size or capability) to successfully implement Digital Forensics Capability Maturity effectively by using the DF-C²M² Body of Knowledge, guidelines, and Assessment tool.

The DF-C²M²' benefits and viability to organisations and practitioners alike has been demonstrated, and the DF-C²M² presents a sustainable model and framework for implementing Capability Maturity in a flexible, cost-effective manner that will appeal to a multitude of organisations regardless of size, regulatory requirements, scope of services, and accreditation status.

The discipline of Digital Forensics has, to date, 'been largely an unregulated area of law, but certification programs combined with self-regulation may be the best means for establishing the profession in the eyes of the courts' (Krause, 2010). The adoption of the DF-C²M² will provide a viable means towards self-regulation, standardisation of requirements to be recognised as a digital forensics examiner, establishing capability maturity as a key business, and quality management focus.

To date, this investigation represents the most extensive research on the subject of digital forensics lab organisational challenges and the applicability of capability maturity within the realm of digital forensics.

The DF-C$^2$M$^2$ presents Digital Forensic organisations and the broader community at large with a unique opportunity to improve and incorporate capability maturity across the People, Processes, and Tools domains of their business, and help address their business drivers and goals.

The DF-C$^2$M$^2$ has proven to be an effective framework through which organisations can more efficiently plan, implement, manage, and optimise their digital forensic laboratories whilst still meeting the pressing business and regulatory drivers, in a cost-effective and timely manner.

The DF-C$^2$M$^2$ will potentially contribute significantly to the first standardised framework for establishing, running, and maintaining digital forensic labs in both law enforcement and commercial environments to help bring the status of digital forensics closer to having the key elements for being recognised as a standardised true forensic discipline.

Analysis of all of the key concerns and needs raised by the majority of digital forensic practitioners and unit managers’ points to one key solution that will enable organisations to better understand their capabilities, limitations, and the best ways to achieve maximum efficiency: that of *Capability Maturity*. Capability Maturity Models have not, to date, been applied to the field of digital forensics in a holistic way that encompasses standards requirements and business needs in a comprehensive management support system.

While the proposed DF-C$^2$M$^2$ model is not a panacea to solve all of the managerial and quality management issues of digital forensic laboratories as presented in this thesis, it provides a key management support system and framework that will enable organisations to meet regulatory and accreditation requirements while achieving capability maturity, and in the process, help management to better visualise and understand their lab’s deficiencies and provide an easy means to measure and improve overall capability maturity and efficiency.

Strategically, although many Digital Forensics practitioners view digital forensics as a forensic science, this ‘science’ lacks a body of knowledge, a standard set of requirements for curricula, training, job titles review, and accreditation of personnel – key requirements for it to be viewed as a true science by the forensic community as a whole.

The lack of minimum required training, and experience requirements for various digital forensics roles, has created major disparities in that one who is ‘qualified’ by their lab as a digital forensic computer examiner may only qualify as a digital forensic technician/engineer in another lab – as witnessed in the Lab Assessments.

These issues within the field of Digital Forensics have only contributed to, and re-enforced, the view amongst the broader scientific community as a whole that Digital Forensics is not a true or recognised forensic science. It is time that the discipline of Digital Forensics becomes a true forensic science, and a chartered profession; the DF-C$^2$M$^2$ provides the first step in helping to fulfil that broader and most important objective.

# APPENDIX A: EVALUATION FORM DEMOGRAPHIC DATA COLLECTED

**Name of Reviewer** : ______________________________________

**Position/Job Title** : ______________________________________

**Number of Years' Experience in Digital Forensics/Legal Frameworks or Standards (if applicable):**

□ 0-3 years □ 4-6 years □ 7 -10 years □ More than 10 years

**Digital Forensics Role:**

□ Digital Forensics Practitioner

□ Digital Forensics Student

□ Digital Forensics Subject Matter Expert

□ Digital Forensics Academic

□ Digital Forensics Lab Manager

□ Other: ______________

**Organisation Name** : ______________________________________

**Accredited Lab:** □ ISO 17025 □ ASCLD-LAB □ None

**Organisation Type**

□ Law Enforcement □ DF-C$^2$M$^2$ Academic

□ Govt/Regulatory □ Commercial Entity

□ National Standards Body □ International Standards

□ Other:

_____________________________________________________

Thank you for your participation in the DF-C$^2$M$^2$ review and your invaluable feedback. Your feedback and comments will remain confidential. Results of the evaluation will be published in due course and your recommendations on how the DF-C$^2$M$^2$ can be improved to be more efficient and sustainable in the long-term are welcome.

Yours sincerely,

**Ebrahim Al Hanaei**

# APPENDIX B: PARTICIPANT CONSENT FORM

## Digital Forensics Comprehensive Capability Maturity Model

**Names of researchers conducting the study:** ______________________________

______________________________________________

**Name of participant:** ______________________________

The purpose of this consent form is to check that you are aware of your rights, understand what will be required of you and agree to take part in the study.

*Please initial each box*

1. I confirm that I have read and understood the Participant Information Sheet (version 1, 19 July 2013) for the above research. □

2. I have had the opportunity to consider the information, ask questions about the research and have had these answered satisfactorily. □

3. I agree to take part in the research and understand that my participation is voluntary. □

4. I understand that I have the right to withdraw from the participation, without giving reasons for this, at any point during the process. □

5. I am satisfied that the information I provide will be treated confidentially by the researchers. □

6. I agree for the sessions to be audio recorded (if applicable). □

7. I agree that quotations from the interviews can be used in the project reports and in other publications (if applicable). I understand that my quotations will be used anonymously. □

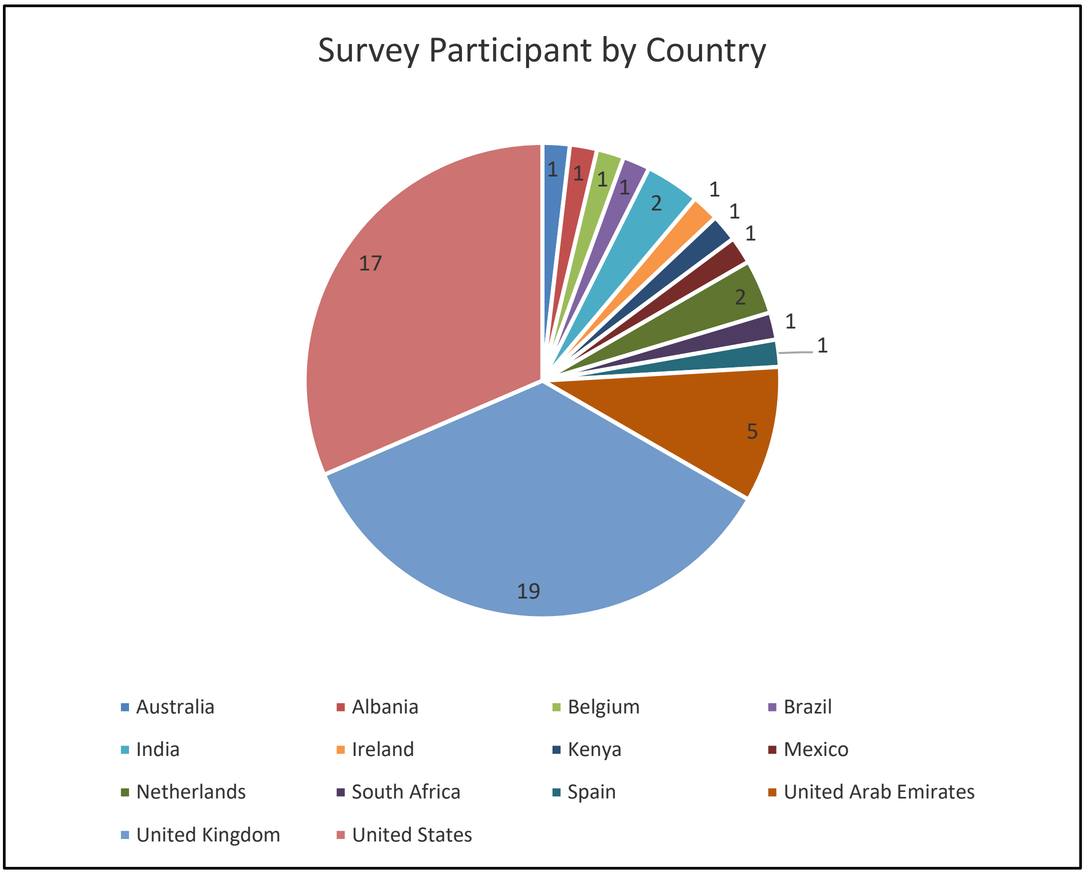
Participant's Signature: ______________________

Researcher's Signature: ______________________

Date: ____________

# APPENDIX C: ONLINE SURVEY EXTRACT FINDINGS

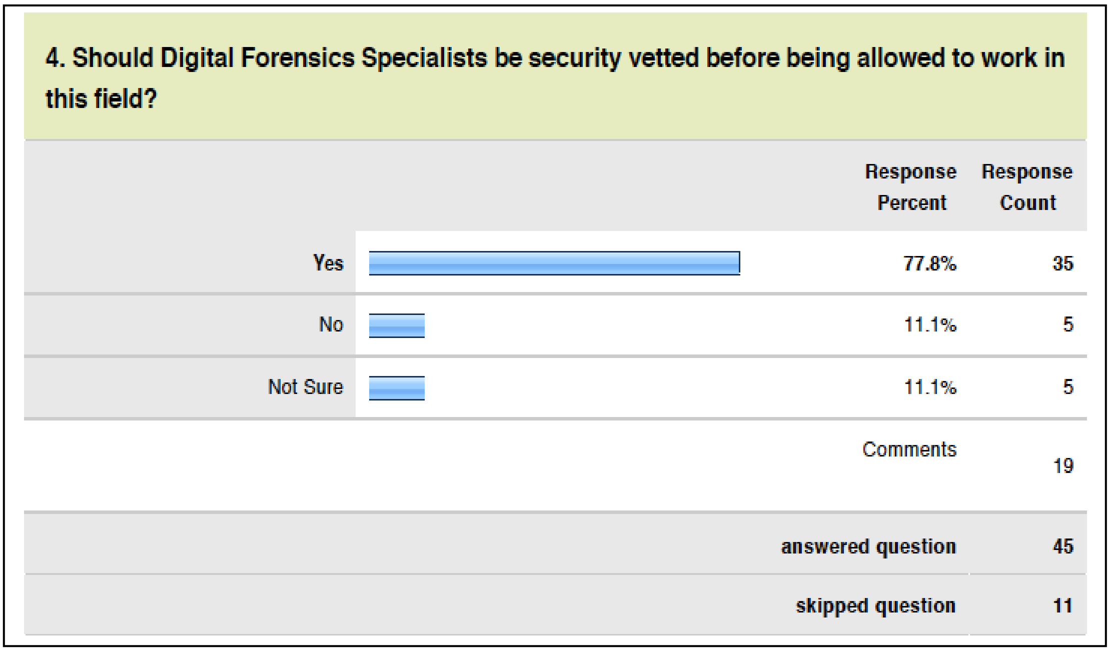
Participants from 14 countries took part in the online survey as shown below:



Questions one to three relate to consent and awareness hence they bear no value for the requirements.

The following paragraphs represent the analysis of the questions from four to forty quantitatively and some qualitative analysis base on the comments on each question.

Q4:



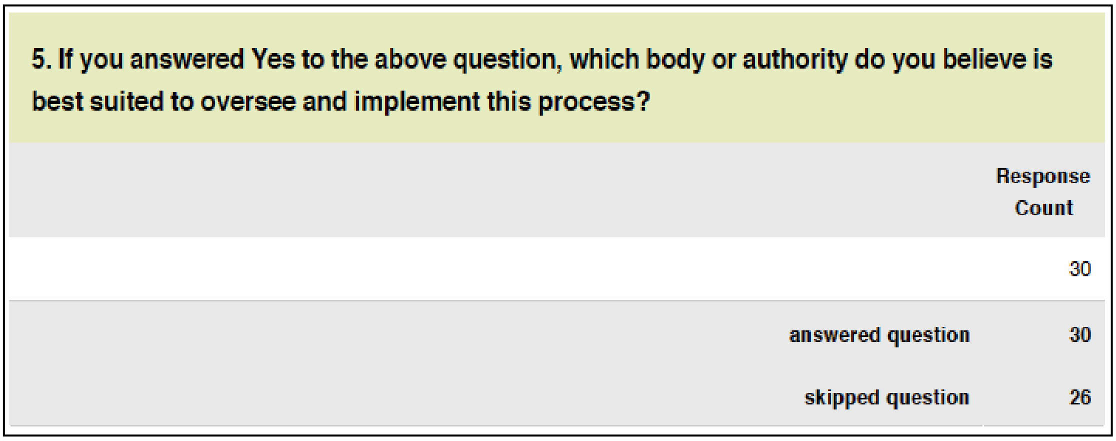
**4. Should Digital Forensics Specialists be security vetted before being allowed to work in this field?**

| | Response Percent | Response Count |
|---|---|---|
| Yes | 77.8% | 35 |
| No | 11.1% | 5 |
| Not Sure | 11.1% | 5 |
| | Comments | 19 |
| | answered question | 45 |
| | skipped question | 11 |

This question was answered by 45 responses, with 77.8% positive, 11.1% negative and 11.1% not sure. This indicated a *clear need for security vetting*.

Looking at the qualitative side of this question the comments given were either explaining the reason and the level of vetting required or defending the status quo. Those who responded negative showed great fear of the security threat to their job or their qualification. Mostly either favouring to earn their living as manipulators of desired results by abusing the data and twisting results, which may not be possible if they are security vetted. So the current lack is useful or none-useful for some specialists, which opens the door for fraud and longer legal procedures by lawyers. Suggestions were given on the level of vetting ranging from just Criminal Records Bureau (CRB) to Security Clearance (SC) and Developed Vetting (DV).

Q5:



**5. If you answered Yes to the above question, which body or authority do you believe is best suited to oversee and implement this process?**

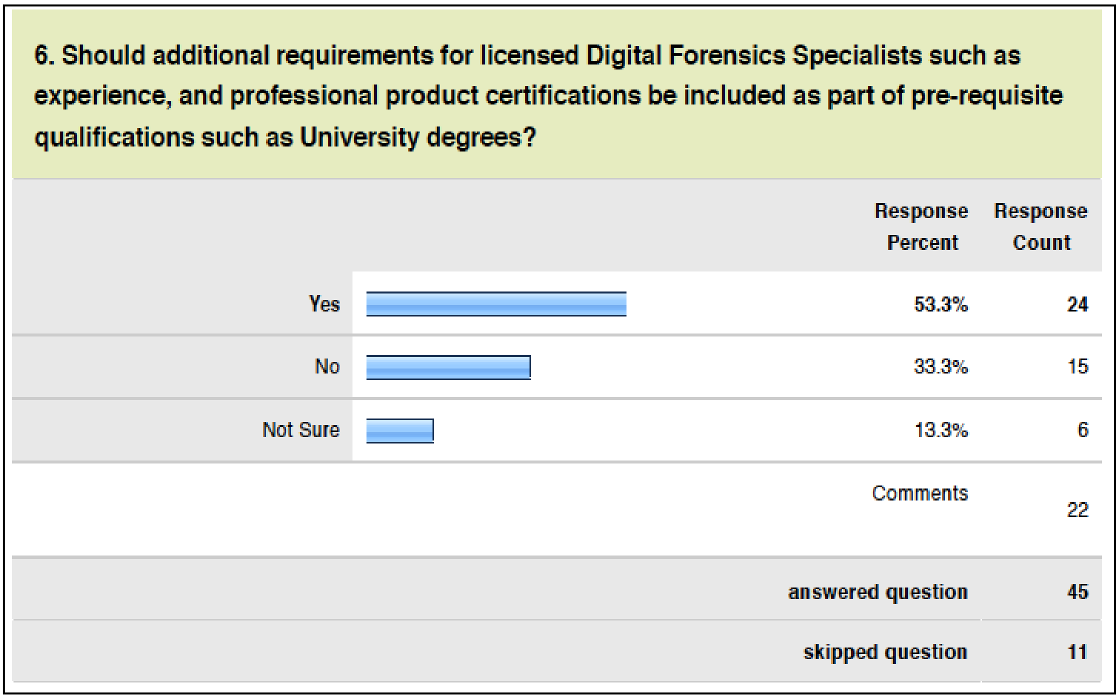
| | Response Count |
|---|---|
| | 30 |
| answered question | 30 |
| skipped question | 26 |

Thirty participants answered this question. Suggestions were various and diverge however; the majority suggests a government security body namely the equivalent of the ministry of interior or the jurisdiction authorities (courts) or both. This makes sense as most of security vetting for other criminal investigators is done at such level of state security bodies. The benefit is lesser legislation requirements for this area of vetting and lesser legal procedures in courts. Samples are shown below:

- CGC security vetting
- A new single uniformed certification body is needed to unify the current tool identification certificates like EnCasE and general certifying bodies for CFCE Such through agents like IACIS.
- Specialized government bodies.
- Special body for commercial organization
- Industry sponsored groups.
- Criminal records Bureau for standard CRB vetting, home office of MoD for higher vetting levels.
- Government, manufacturers, training partners, suppliers and police authorities
- Local state authorities set standards using qualified.
- State security department and social support department
- Organizational security clearance authorities – meaning the ministry of interior.
- Ministry of interior
- International specialized organization
- Low enforcement or state security

- National forensics regulator
- Local and / or state forensics boards
- A professional organization such as CDFS
- The employing authority – police will use their own vetting.
- Local / international courts
- A regulatory body that have jurisdiction
- Police certificates.
- Home office/ ministry of interior
- An international governing body with global geographical representatives that oversee experts and specialists. However, they assume that those governors have just experience criteria of 10 years.
- Local state or federal security clearances in the jurisdiction.

Q6:



**6. Should additional requirements for licensed Digital Forensics Specialists such as experience, and professional product certifications be included as part of pre-requisite qualifications such as University degrees?**

| | Response Percent | Response Count |
|---|---|---|
| Yes | 53.3% | 24 |
| No | 33.3% | 15 |
| Not Sure | 13.3% | 6 |
| | Comments | 22 |
| | answered question | 45 |
| | skipped question | 11 |

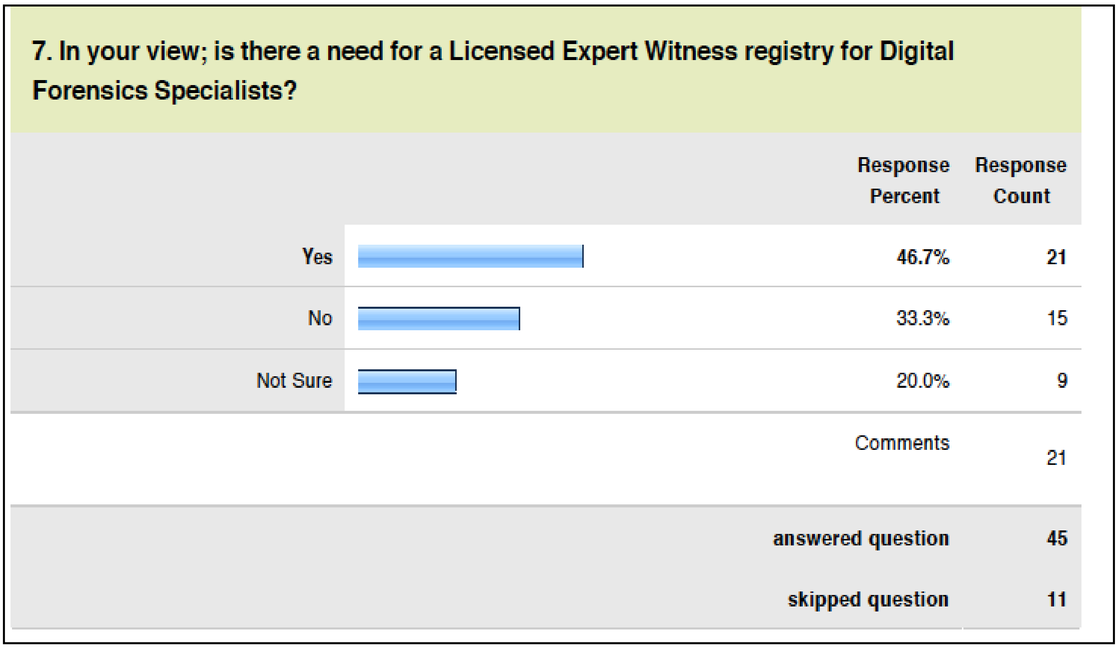
Forty-five participants, with 53.3% positive, 33.3% negative and 13.3% answered this question not sure. This indicated a clear need for *additional requirements for licensing Digital Forensics specialists*. However, the significant rejection may indicate some have the tendency to accept current practices that is based on technical training and experience, or the fear from job loss as will be detailed in the qualitative analysis of the comments.

Looking at the qualitative side of this question, the comments given were diverse again specially among those who were rejecting the idea. It reflected job security worries and the need to use experience standardized through qualifying exams rather than a degree. However, using a qualifying body such as NVQ in the UK would help mitigate those worries. A competency assessment is more important. However, in conclusion the majority are in agreement with the need for a university degree followed by experience or professional qualifications of timed validity to cover for technology change. The following is a summary of the comments given.

- No university degree is required, experience is what matters
- Both qualification and experience are needed
- Qualifications should be standardized and available to police and non-police personnel
- A standard of competency is required
- Academic qualifications give credibility, but prior experience is important
- Proper training is important
- Range of specifications is so broad to be included in one qualification
- University degree will not be a qualifier. Training and experience are more important.
- IT degree is important
- A start is needed
- University degree is not a pre-requisite. Assessment of the skills is enough
- ISO 17025 requires competency testing
- Skill test and apprenticeship would be the minimum standard
- Currently specialists are interested in experience for their CV
- Currently half packed university graduates seek experience for their CV
- At least a university degree
- We should aim at digital forensic scientists
- Degrees are nice to have, but experience and skill is important
- Multiple certificates to cover various products

These comments reflect clearly that the participants that have resistance to the idea of a degree are enjoying some kind of job competence and security based on the current system of training and certification. In addition, the current certification system does not require a degree, hence suggesting it would represent a hurdle to those currently certified and working.

Q7:



7. In your view; is there a need for a Licensed Expert Witness registry for Digital Forensics Specialists?

| | | Response Percent | Response Count |
|---|---|---|---|
| Yes | | 46.7% | 21 |
| No | | 33.3% | 15 |
| Not Sure | | 20.0% | 9 |
| | | Comments | 21 |
| | | answered question | 45 |
| | | skipped question | 11 |

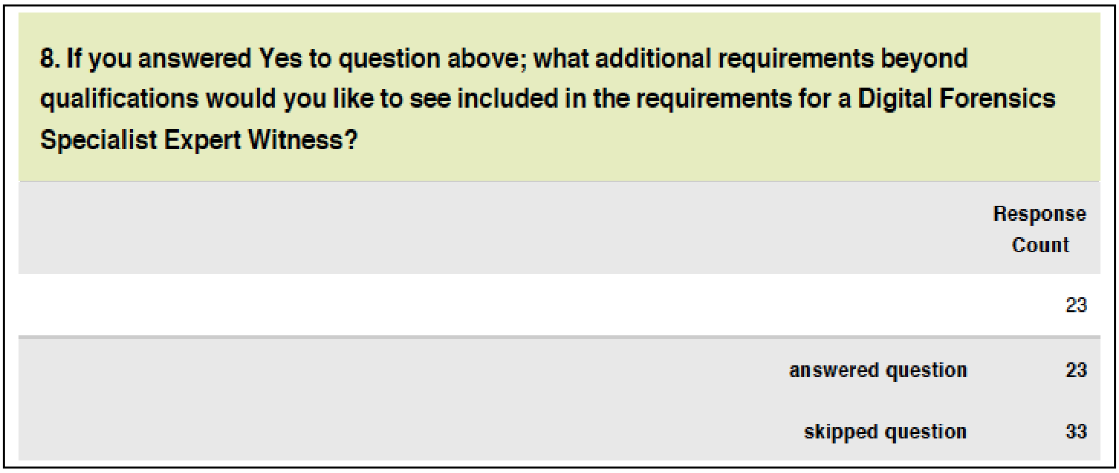
Forty-five participants, with 46.7% positive, 33.3% negative and 20%, answered this question not sure. This indicated a relatively significant *need for additional requirements for licensed Exert Witness Registry for Digital Forensics specialists*. In addition, the one third that is rejecting this requirement indicates a level of resistance that needs exploration.

Looking at the qualitative side of this question, the comments given were diverse again specially among those who were rejecting the idea. It is consolidating the fact that a formal recognition body is seen as a threat to current witnesses. Some opponents rejected the idea if it will exclude unlisted experts and saw it as a money collection exercise that is costly for small companies.  It is also seen as a mission impossible as participants against it think it is difficult to decide on a reference body for standardizing and granting this licence and keeping a registry. Some claimed that by being employed by an organization that is ISO 17025 certified they become automatically accredited.

Proponents of this requirement see it as good for ensuring competence and ethical behaviour of witnesses as they assume paid-for witnesses' charlatans will disappear. It will also stop picking expert witnesses at will thus opening doors for corruption and intimidation.

There is also a language dilemma and regulation dilemma between, for example, European and USA regulatory and licensing traditions that may slow down creating an international *licensed Exert Witness Registry*. Bureaucracy was seen as a major obstacle especially due to lawyers' practices.

Q8:



**8. If you answered Yes to question above; what additional requirements beyond qualifications would you like to see included in the requirements for a Digital Forensics Specialist Expert Witness?**

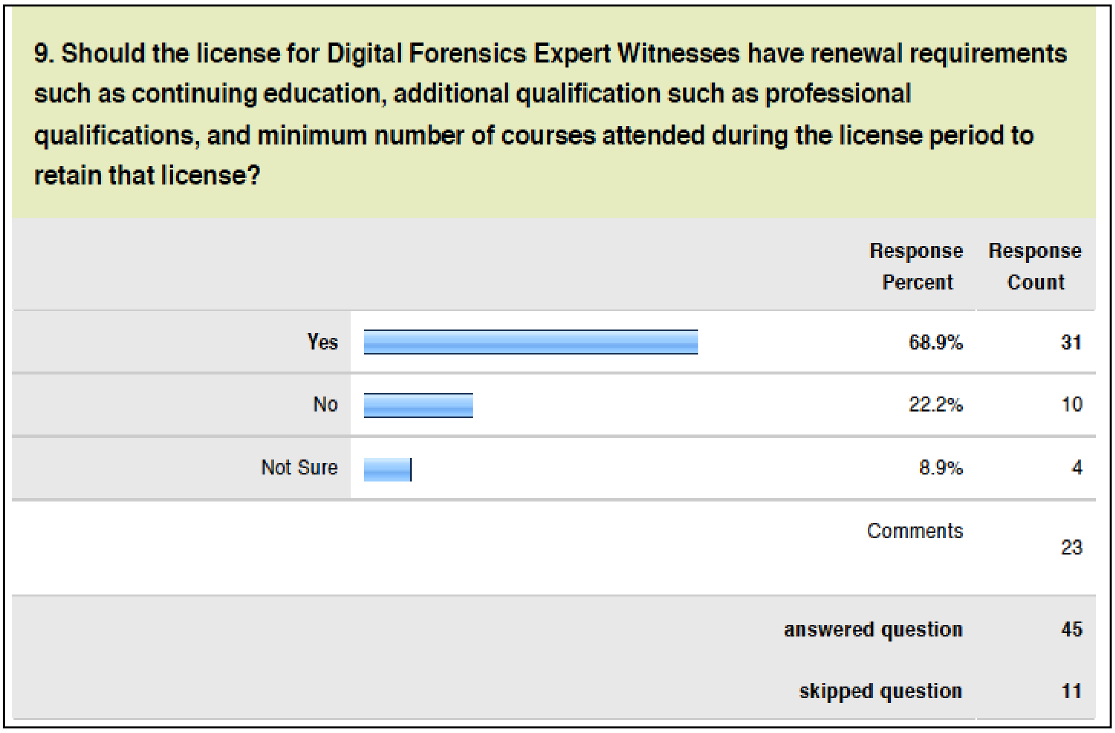
| | Response Count |
|---|---|
| | 23 |
| answered question | 23 |
| skipped question | 33 |

This question was answered by twenty-three participants. The additional requirements proposed can be summarized as follows:

- An account of experience
- Evidence-based Competency assessment for licensing through an approved body (to cover practical experience)
- Low cost or free licensing
- Maintenance of competency and continuing education to cope with change in technology (licenses should have a validity period)
- Examiners should be from a third party not from within the security agency
- In USA, only courts determine who is an expert.
- Absence of criminal record and sound mental health must be part of the criteria
- Knowledge of law, familiarity with legal procedures, absence of criminal record, and sound mental health
- Number of witnesses before a court!
- CV, peer reviews, board certification,

- Meet the rules of expert witness in Australia, Canada, USA, and England where a combination of education, training, and experience is necessary.
- Experience (min 5 years), Presentation skills, Report Writing skills and more court training
- Basic legal training regarding the role of an expert witness

Q9:



**9. Should the license for Digital Forensics Expert Witnesses have renewal requirements such as continuing education, additional qualification such as professional qualifications, and minimum number of courses attended during the license period to retain that license?**

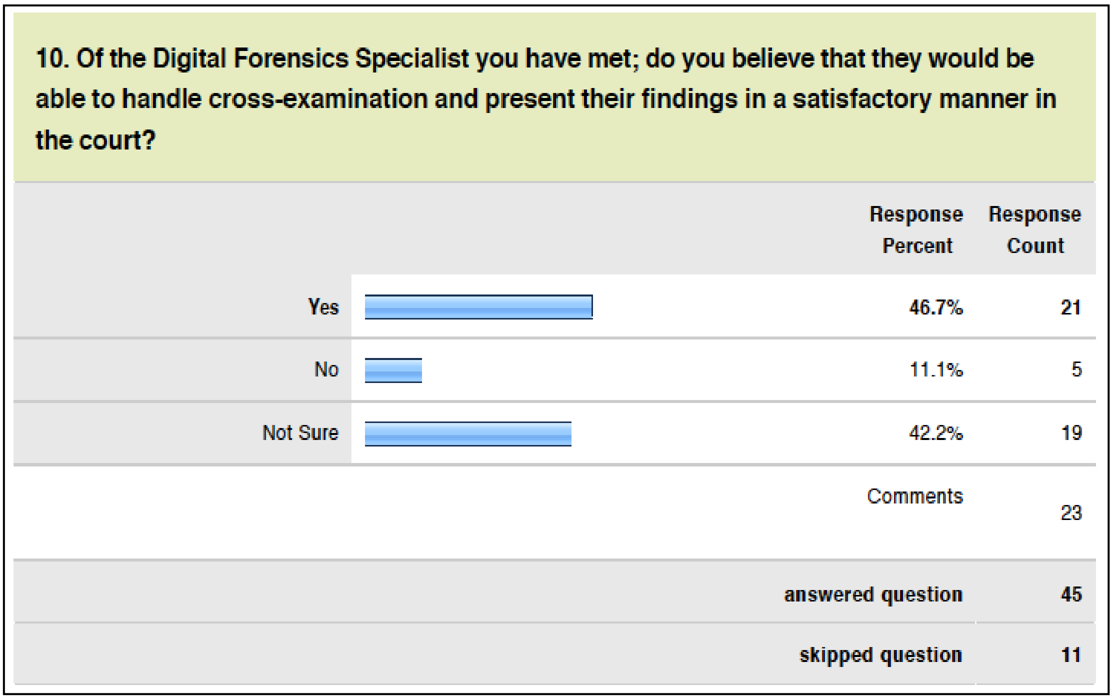
| | | Response Percent | Response Count |
|---|---|---|---|
| Yes | | 68.9% | 31 |
| No | | 22.2% | 10 |
| Not Sure | | 8.9% | 4 |
| | | Comments | 23 |
| | | answered question | 45 |
| | | skipped question | 11 |

Forty-five participants responded, with 68.9% positive, 22.2% negative and 8.9%, answered this question not sure. This indicated a clear need for *renewable requirements for licensed Exert Witness* Registry for Digital Forensics specialists.

Looking at the qualitative side of this question, the comments given were diverse again specially among those who were rejecting the idea where comments aimed at employer bearing the cost with more generosity and less frequent renewals to avoid a “points gathering exercise”. A sound comment was regarding continuing education experts, who will qualify them and renew their licenses? Some indicated that such profession does not have licensing in USA.

Proponents were concerned about the change in technology and the need to update policies to cope. They suggested attending exhibitions, conferences and refresher competency-based courses and assessments. A proposal was to refresh every 3-5 years.

Q10:



**10. Of the Digital Forensics Specialist you have met; do you believe that they would be able to handle cross-examination and present their findings in a satisfactory manner in the court?**

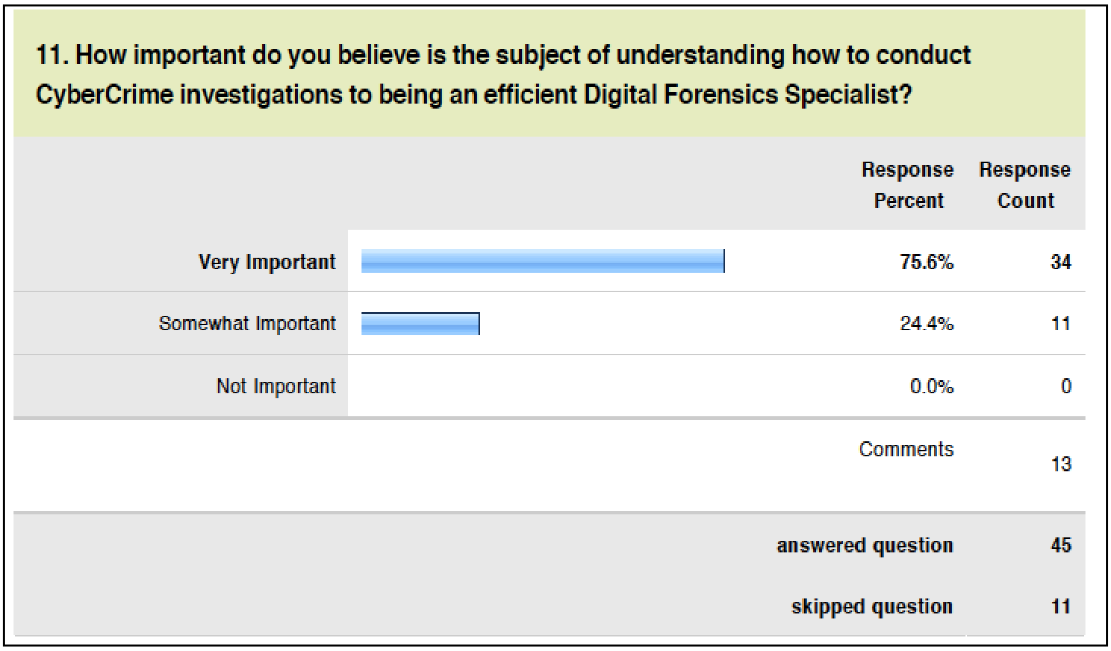
| | | Response Percent | Response Count |
|---|---|---|---|
| Yes | | 46.7% | 21 |
| No | | 11.1% | 5 |
| Not Sure | | 42.2% | 19 |
| | | Comments | 23 |
| | | **answered question** | **45** |
| | | **skipped question** | **11** |

Forty-five participants responded, with 46.7% positive, 11.1% negative and 42.2%, answered this question not sure. This indicated a rather clear positive opinion that digital forensic experts would be able to *handle cross-examination and present findings satisfactorily*. The significant "not sure" percentage shows a need for qualification or training.

Looking at the qualitative side of this question, the comments given were diverse again. It is amazing despite the approval of training, qualification and licensing that judging peers in the profession did manifest itself in a direct manner. Those who expressed not sure, would be embarrassed from saying NO in this question despite they said the need for training and development up to a unified standard in previous questions. A sense of security might be behind such behaviour.

Most comments were neutral or balanced dividing the probability equally between yes and no. A good group was directly pointing at lack of the skills. Moreover, many were avoiding confronting the issue.

Q11:



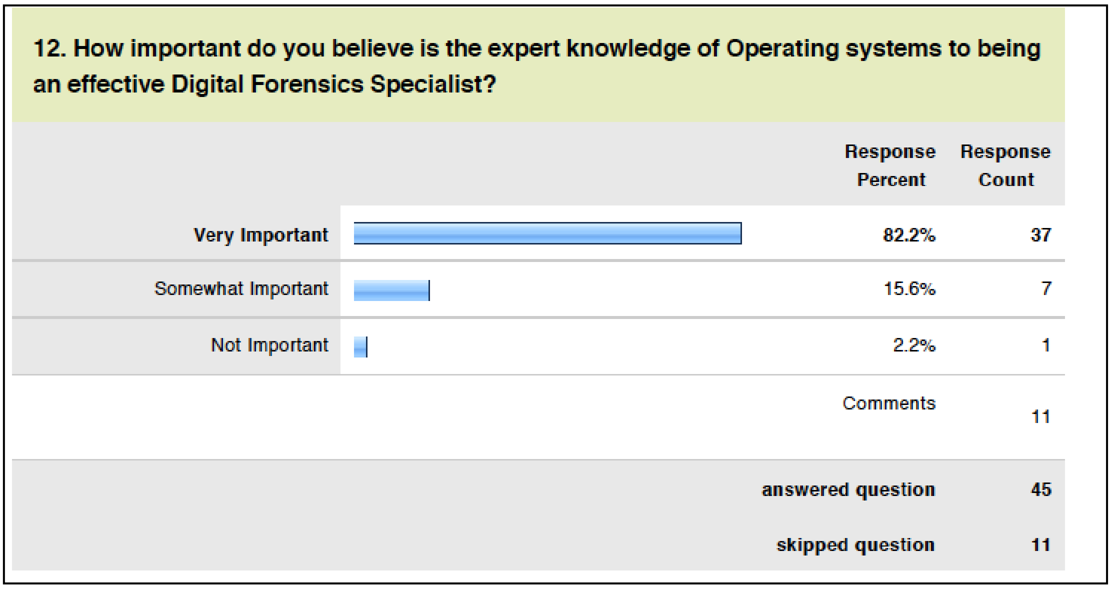
**11. How important do you believe is the subject of understanding how to conduct CyberCrime investigations to being an efficient Digital Forensics Specialist?**

| | | Response Percent | Response Count |
|---|---|---|---|
| Very Important | | 75.6% | 34 |
| Somewhat Important | | 24.4% | 11 |
| Not Important | | 0.0% | 0 |
| | | Comments | 13 |
| | | answered question | 45 |
| | | skipped question | 11 |

Forty-five participants responded, with 75.6% very important, 24.4% rather important and 0% answered this question not important. This indicated a rather clear positive opinion that digital forensic specialists need to *understand cybercrime investigation to become efficient.*

Most of the qualitative comments supported the importance of IT background and one comment mentioned that in Germany IT-personnel are being trained on law rather than training police officers on IT to handle cybercrime and DF. From the bio data of participants, the majority have law enforcement background; hence, the IT issue is significant more than the investigation skill.

Q12:



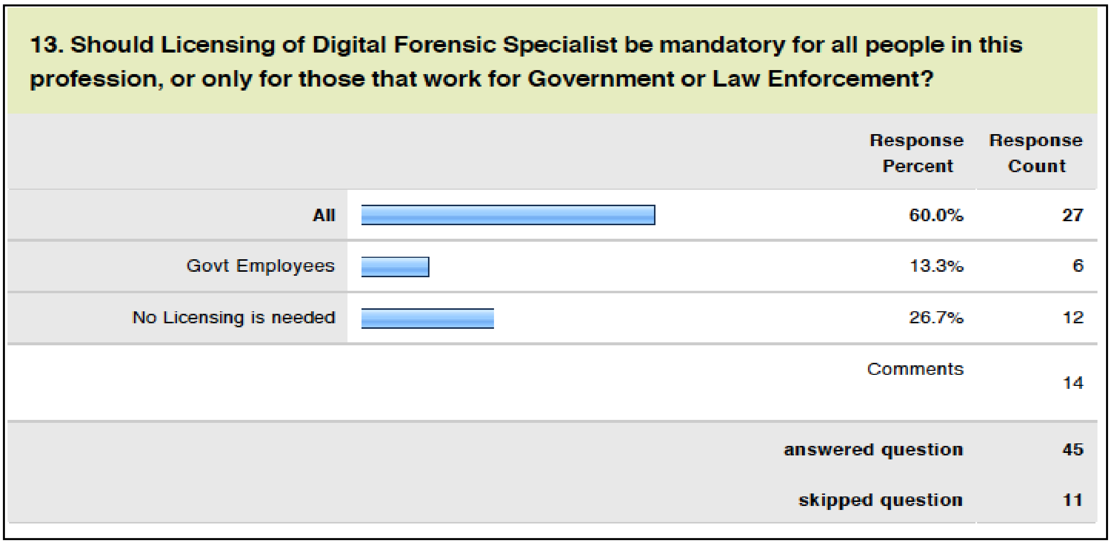
12. How important do you believe is the expert knowledge of Operating systems to being an effective Digital Forensics Specialist?

| | Response Percent | Response Count |
|---|---|---|
| **Very Important** | 82.2% | 37 |
| Somewhat Important | 15.6% | 7 |
| Not Important | 2.2% | 1 |
| | Comments | 11 |
| | **answered question** | **45** |
| | **skipped question** | **11** |

Forty-five participants responded, with 82.2% very important, 15.6% rather important and 2.2% answered this question not important. This indicated the importance of expert knowledge of Operating systems for efficient digital forensic specialists.

On the Qualitative side of the responses, the majority of the comments endorsed the statistics directly. The need for operating system knowledge is obviously seen by many as part of the essential expertise.

Q13:



13. Should Licensing of Digital Forensic Specialist be mandatory for all people in this profession, or only for those that work for Government or Law Enforcement?

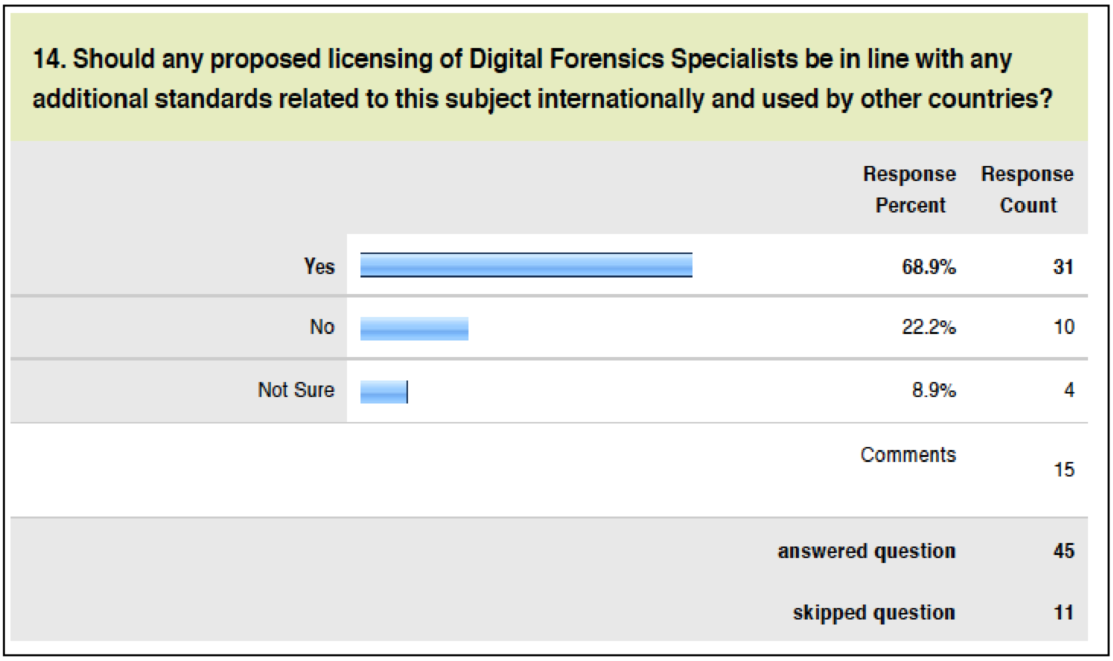
| | Response Percent | Response Count |
|---|---|---|
| **All** | 60.0% | 27 |
| Govt Employees | 13.3% | 6 |
| No Licensing is needed | 26.7% | 12 |
| | Comments | 14 |
| | **answered question** | **45** |
| | **skipped question** | **11** |

Forty-five participants responded, with 60% suggesting all specialists should be licensed, 13.3% suggesting only government employees and 26.7%, rejected licensing.

This indicated a rather clear positive opinion that *Licensing of Digital Forensic Specialist be mandatory*. It was shocking to find responses that rejected the idea; however, it augments the previous finding that some current specialists are scary of the idea of having to be licensed.

On the Qualitative, side findings showed the need for standardizing licensing for all specialists. A couple of comments highlighted the link of such standards to training and competence assessment.

Q14:



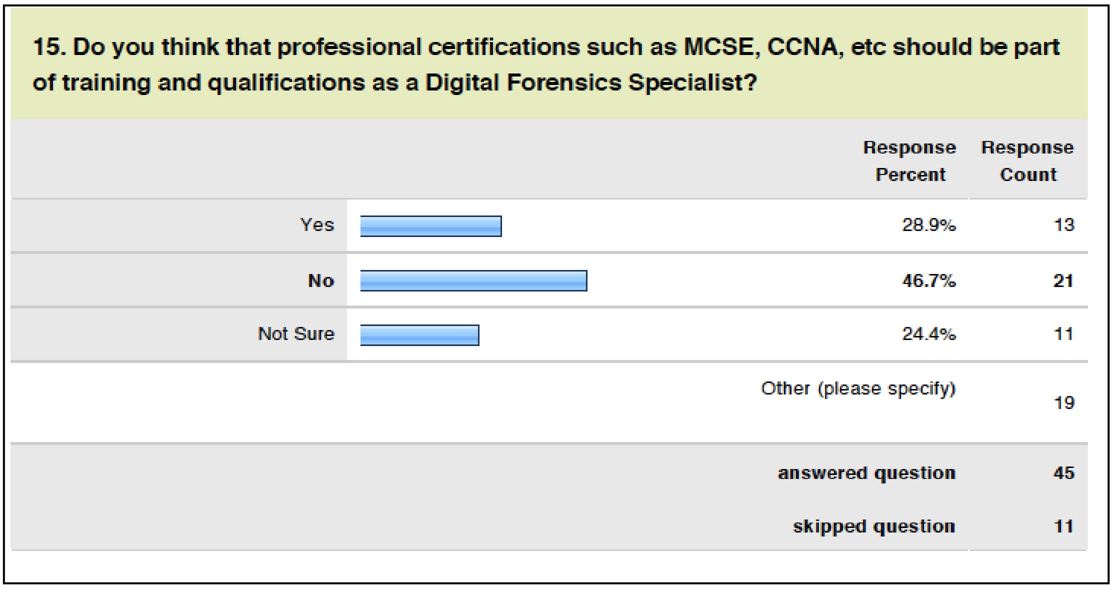
**14. Should any proposed licensing of Digital Forensics Specialists be in line with any additional standards related to this subject internationally and used by other countries?**

| | Response Percent | Response Count |
|---|---|---|
| Yes | 68.9% | 31 |
| No | 22.2% | 10 |
| Not Sure | 8.9% | 4 |
| | Comments | 15 |
| | **answered question** | **45** |
| | **skipped question** | **11** |

Forty-five participants responded, with 68.9% positive, 22.2% negative and 8.9% answered this question not sure. This indicated a rather positive opinion that *Digital Forensic Specialists licensing should be in line with international standards and used by other countries*.

The Qualitative analysis of comments shows a display of some existing international and country specific standards, which makes the quest of unified standard valid. However, this may face issues with geographical difference in legislation. A suggested minimum requirement standard is proposed.

Q15:



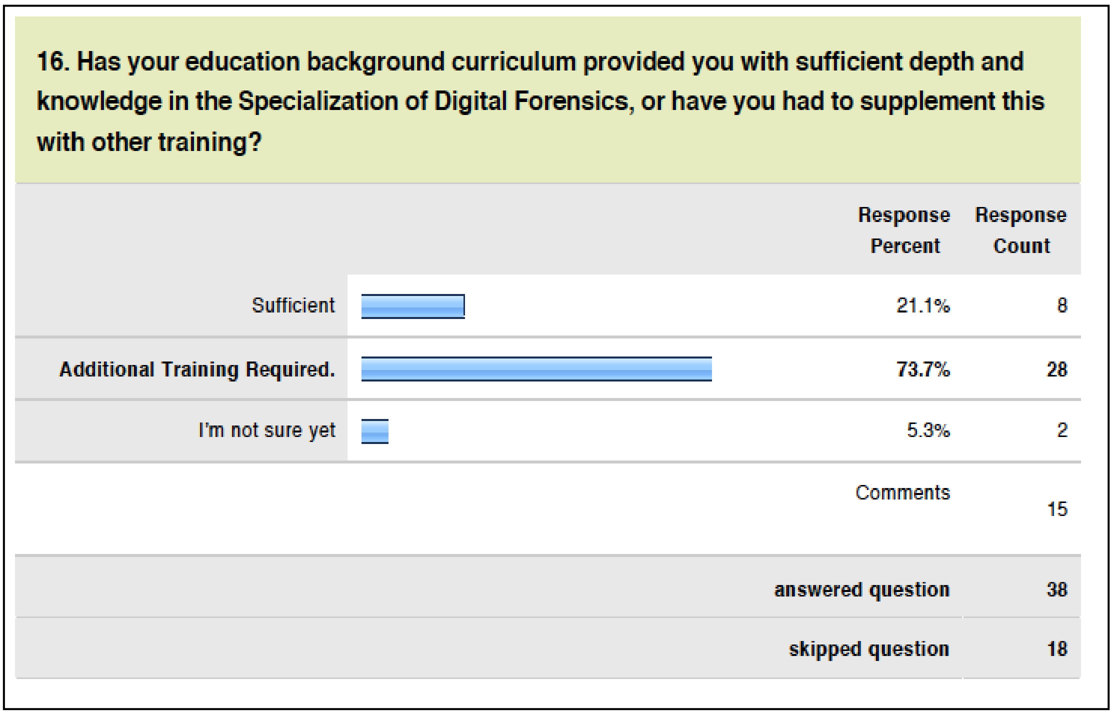
**15. Do you think that professional certifications such as MCSE, CCNA, etc should be part of training and qualifications as a Digital Forensics Specialist?**

|  | Response Percent | Response Count |
|---|---|---|
| Yes | 28.9% | 13 |
| No | 46.7% | 21 |
| Not Sure | 24.4% | 11 |
| Other (please specify) |  | 19 |
| answered question |  | 45 |
| skipped question |  | 11 |

Forty-five participants responded, with 28.9% positive, 46.7% negative and 24.4% answered this question not sure. This indicated a rather negative opinion that MCSE, CCNA, etc. should be part of training and qualification of *Digital Forensic Specialists*. This result is rather shocking as it shows great fear of getting into an area of learning that would be difficult for most of the current specialists.

Qualitative analysis of the comments on this question shows a great deal of resistance. However, a very important recurrent remark noted the importance of targeting such types of IT certification to types of specialists. For example, a network DFS should have a CCNA. The comments specified in detail types of certification required. This showed significant contradiction between the quantitative and qualitative findings.

Q16:



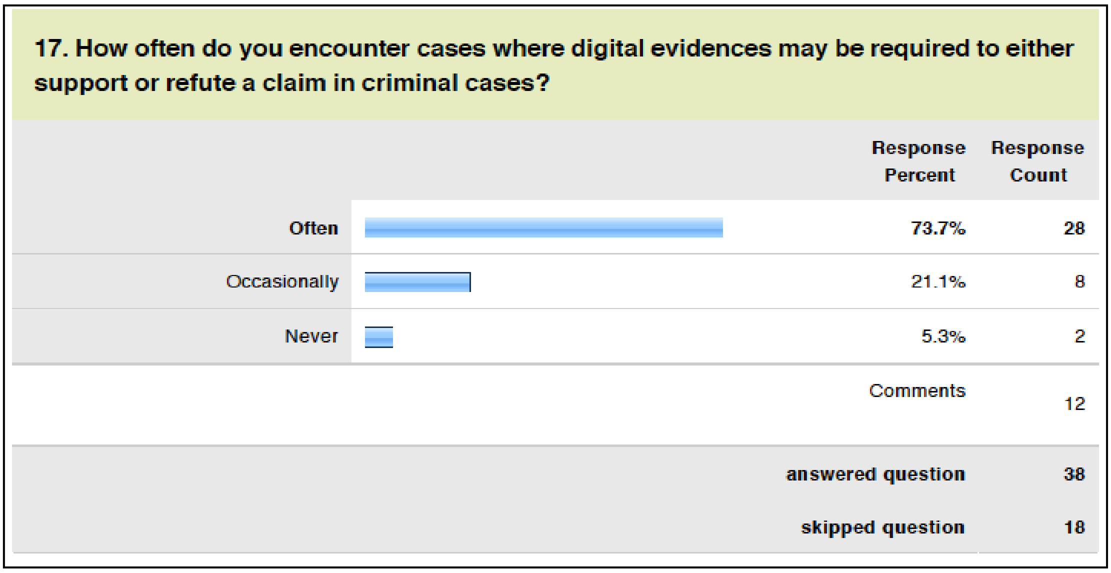
16. Has your education background curriculum provided you with sufficient depth and knowledge in the Specialization of Digital Forensics, or have you had to supplement this with other training?

| | Response Percent | Response Count |
|---|---|---|
| Sufficient | 21.1% | 8 |
| **Additional Training Required.** | **73.7%** | **28** |
| I'm not sure yet | 5.3% | 2 |
| | Comments | 15 |
| | **answered question** | **38** |
| | **skipped question** | **18** |

Thirty-eight participants responded, with 21.1% considering previous education sufficient, 73.7% indicated additional training is required and only 5.3% answered this question not sure. This indicated a rather positive opinion that *Digital Forensic Specialists should have additional specialized training*. This augments the findings in previous questions that a standard for qualification, licensing and training is required.

Qualitative analysis of the comments varied from having M.sc degrees in the subject matters of digital forensics or in IT. This question shows the need for a standard that meets the requirements of the profession. A separate discipline is clearly needed. The width and breadth of the discipline links IT, forensics and investigation and it is obvious that various levels of competence will be required in a model.

Q17:



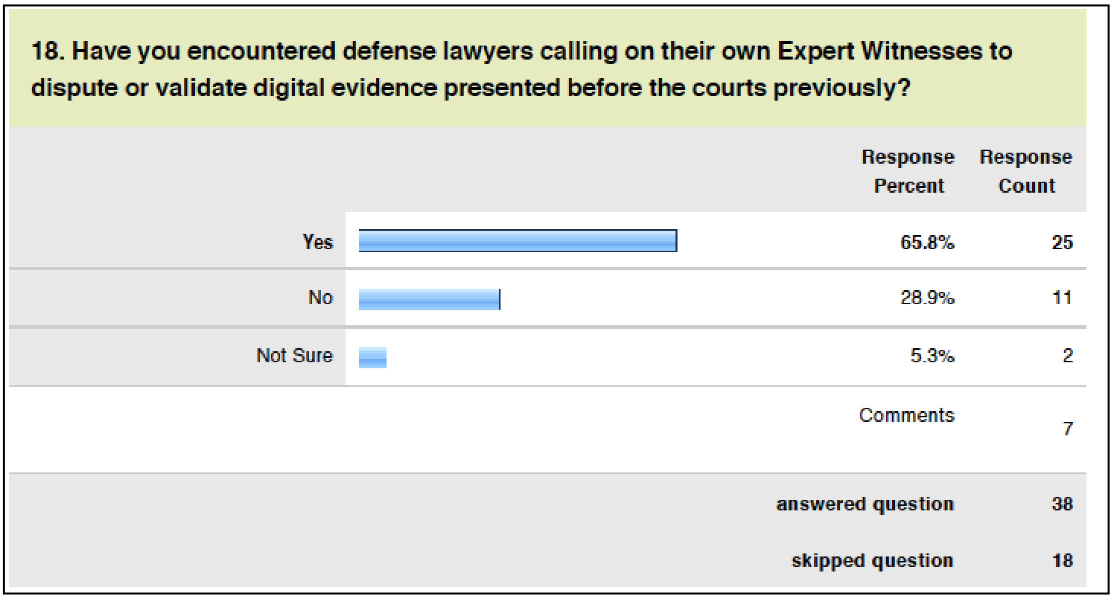
**17. How often do you encounter cases where digital evidences may be required to either support or refute a claim in criminal cases?**

| | Response Percent | Response Count |
|---|---|---|
| Often | 73.7% | 28 |
| Occasionally | 21.1% | 8 |
| Never | 5.3% | 2 |
| Comments | | 12 |
| answered question | | 38 |
| skipped question | | 18 |

Thirty-eight participants responded, with 73.7% considering the digital evidence “often” required 21.1% indicated occasional need and only 5.3%, answered this question as never needed. This indicated a rather positive opinion *digital evidences* are becoming of great importance.

The Qualitative analysis of the comments clarified cases where it became seriously needed, like murder cases and when the Cybercrime laws are enforced in a country.

Q18:



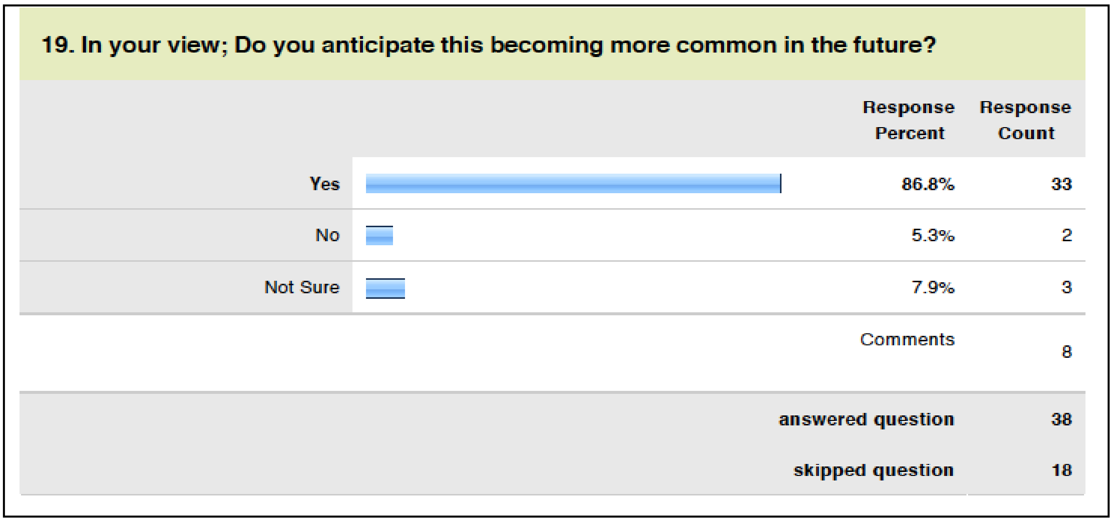
**18. Have you encountered defense lawyers calling on their own Expert Witnesses to dispute or validate digital evidence presented before the courts previously?**

| | | Response Percent | Response Count |
|---|---|---|---|
| Yes | | 65.8% | 25 |
| No | | 28.9% | 11 |
| Not Sure | | 5.3% | 2 |
| | | Comments | 7 |
| | | answered question | 38 |
| | | skipped question | 18 |

Thirty-eight participants responded, with 65.8% positive, 28.9% negative and 5.3%, answered this question not sure. This indicates a clear existence of cases where *Expert Witness* were needed for defence lawyers.

Qualitative analysis of the comments revealed occasions where it was needed either by the participant or by a peer. However, due to lawyers' ignorance of IT technical knowledge they may fall in erroneous choice of witnesses.

Q19:

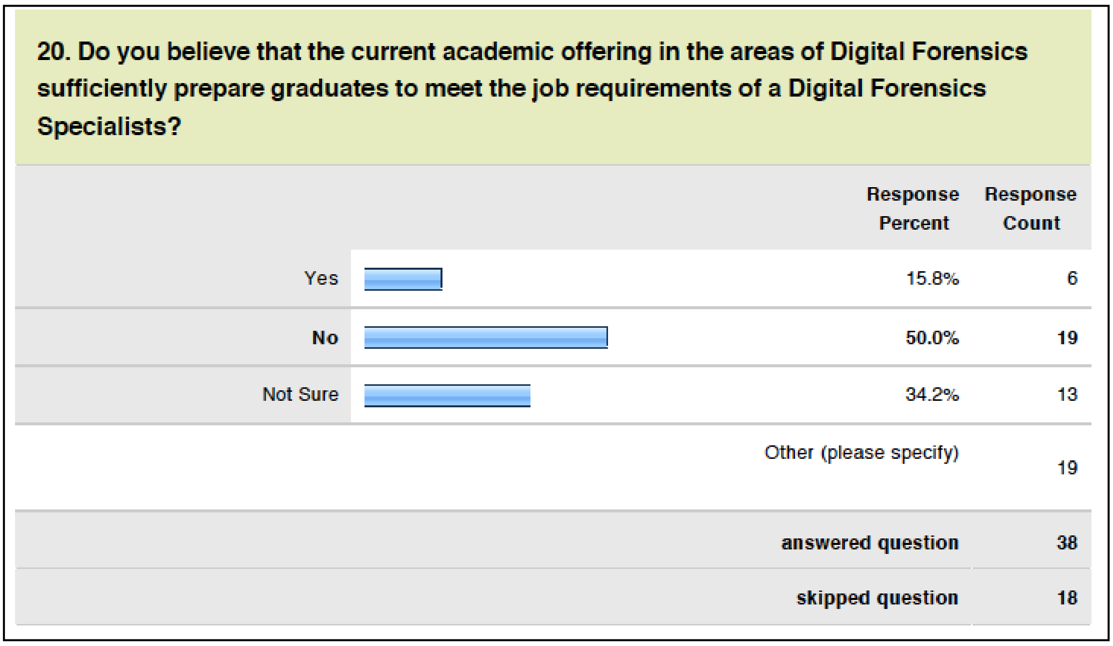


**19. In your view; Do you anticipate this becoming more common in the future?**

| | Response Percent | Response Count |
|---|---|---|
| Yes | 86.8% | 33 |
| No | 5.3% | 2 |
| Not Sure | 7.9% | 3 |
| Comments | | 8 |
| answered question | | 38 |
| skipped question | | 18 |

Thirty-eight participants responded, with 86.8% positive, 5.3% negative and 7.9% answered this question not sure. This indicates a clear requirement for Expert Witness for defence lawyers in the future. Qualitative analysis of the comments revealed that the need exist now and showed some worries about the cost.

Q20:



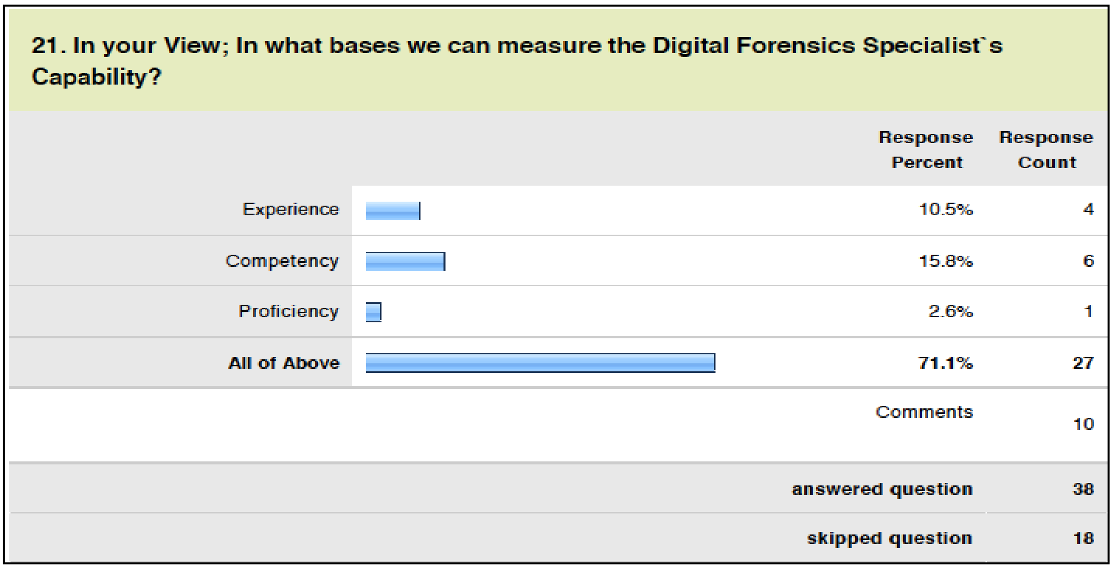
**20. Do you believe that the current academic offering in the areas of Digital Forensics sufficiently prepare graduates to meet the job requirements of a Digital Forensics Specialists?**

| | Response Percent | Response Count |
|---|---|---|
| Yes | 15.8% | 6 |
| No | 50.0% | 19 |
| Not Sure | 34.2% | 13 |
| Other (please specify) | | 19 |
| answered question | | 38 |
| skipped question | | 18 |

Thirty-eight participants responded, with 15.8% positive, 50.0% negative and 34.2% answered this question not sure. This indicates a clear need for *academic offerings* major change to meet the Digital Forensics Specialist discipline requirements.

Qualitative analysis of the comments revealed the need to focus on experience, mentoring, practical work and use of case studies. The comments also indicated lack of sufficiency of the knowledge and skill content of current DF education systems.

Q21:



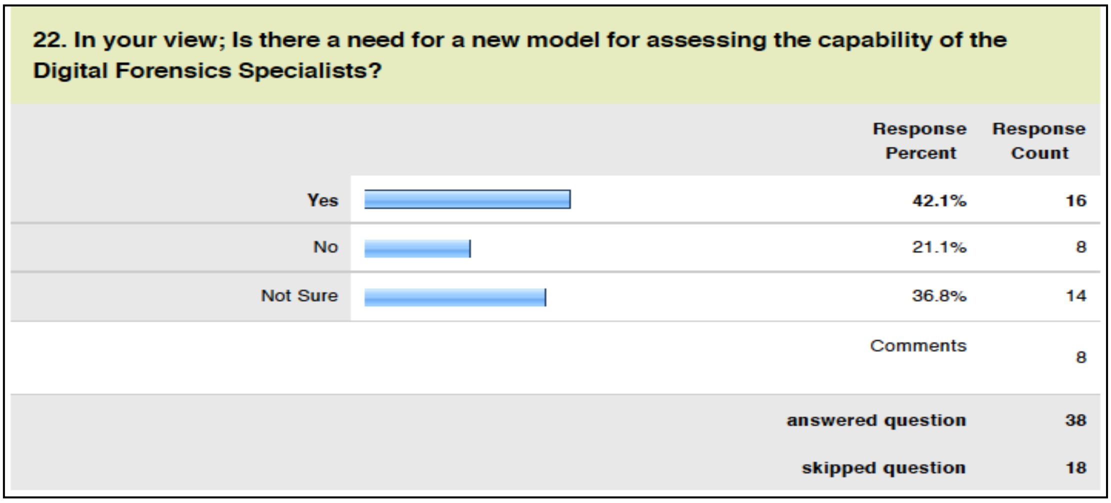
21. In your View; In what bases we can measure the Digital Forensics Specialist`s Capability?

| | Response Percent | Response Count |
|---|---|---|
| Experience | 10.5% | 4 |
| Competency | 15.8% | 6 |
| Proficiency | 2.6% | 1 |
| **All of Above** | **71.1%** | **27** |
| | Comments | 10 |
| | **answered question** | **38** |
| | **skipped question** | **18** |

Thirty-eight participants responded, with 10.5% recommended Experience, 15.8% recommended competency and 2.6%, recommended Proficiency while 71.1% recommended experience, competency and proficiency. This indicates a clear requirement for competency and experience. These feeds into the so far obvious need for education, assessment, and certification which together lead to the capability.

Qualitative analysis of the comments revealed that competency and experience are the two dominant factors leading to capability.

Q22:



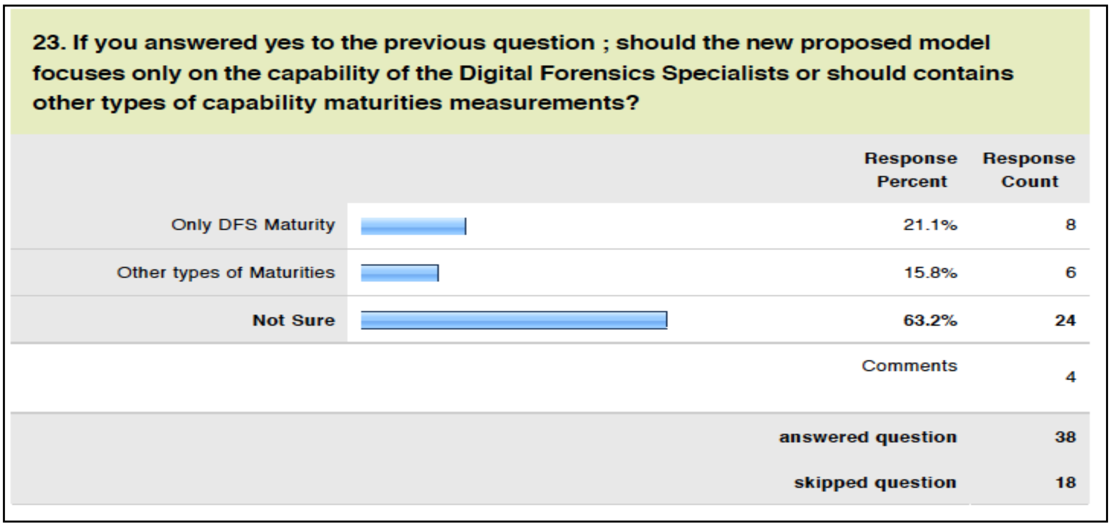
22. In your view; Is there a need for a new model for assessing the capability of the Digital Forensics Specialists?

| | Response Percent | Response Count |
|---|---|---|
| Yes | 42.1% | 16 |
| No | 21.1% | 8 |
| Not Sure | 36.8% | 14 |
| | Comments | 8 |
| | answered question | 38 |
| | skipped question | 18 |

Thirty-eight participants responded, with 42.1% positive, 21.1% negative and 36.8% answered this question not sure. This indicates a rather clear need for a *New Model for Assessing the Digital Forensics Specialist Capability*.

Qualitative analysis of the comments revealed lack of understanding of the term Model and confusion over the meaning of a model and the meaning of standard. So, reaching capability to many will not be easily understood as based on a modelling endeavour for competence and performance in the profession.

Q23:



23. If you answered yes to the previous question ; should the new proposed model focuses only on the capability of the Digital Forensics Specialists or should contains other types of capability maturities measurements?

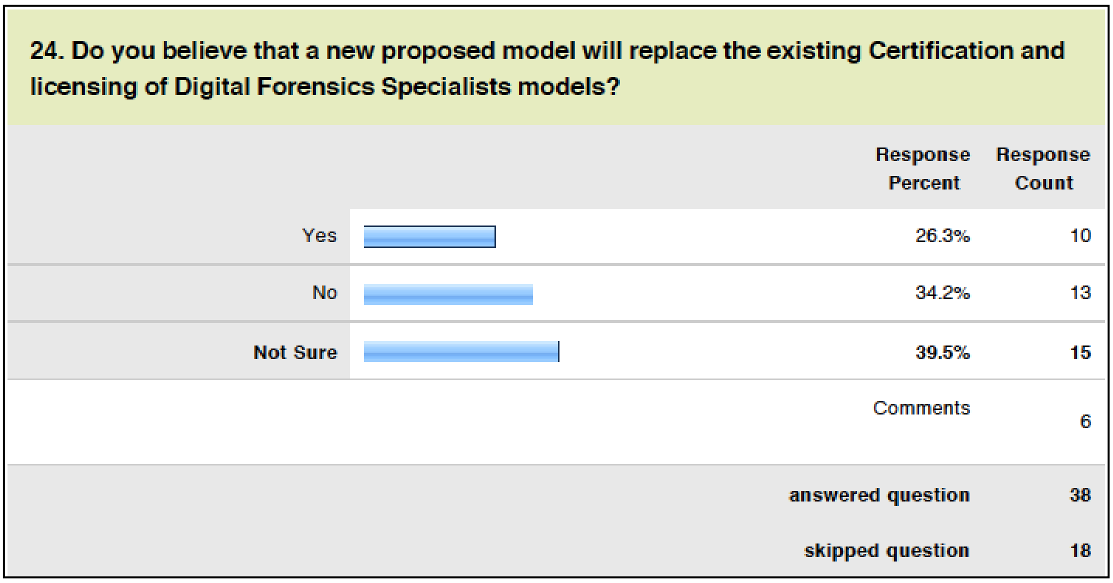
| | Response Percent | Response Count |
|---|---|---|
| Only DFS Maturity | 21.1% | 8 |
| Other types of Maturities | 15.8% | 6 |
| Not Sure | 63.2% | 24 |
| | Comments | 4 |
| | answered question | 38 |
| | skipped question | 18 |

Thirty-eight participants responded, with 21.1% recommended Only DFS maturity, 15.8% recommended other types of maturity and 63.2%, were not sure. This indicates confused majority.  Which would be attributed to misunderstanding of the terms of

Model and Maturity, or attributed to resistance to the idea of assessing and enforcing through a new capability model, that would jeopardise the job security of some current specialists?

Qualitative analysis of the comments revealed fear of new approaches and the term “model” was confusing to those who sought a renewed approach as well as those who did not want any change and prefer the status quo. This shows that there is a probability of lack of a comprehensive body of knowledge and skills that covers the area of professional digital forensics.

<u>Q24:</u>



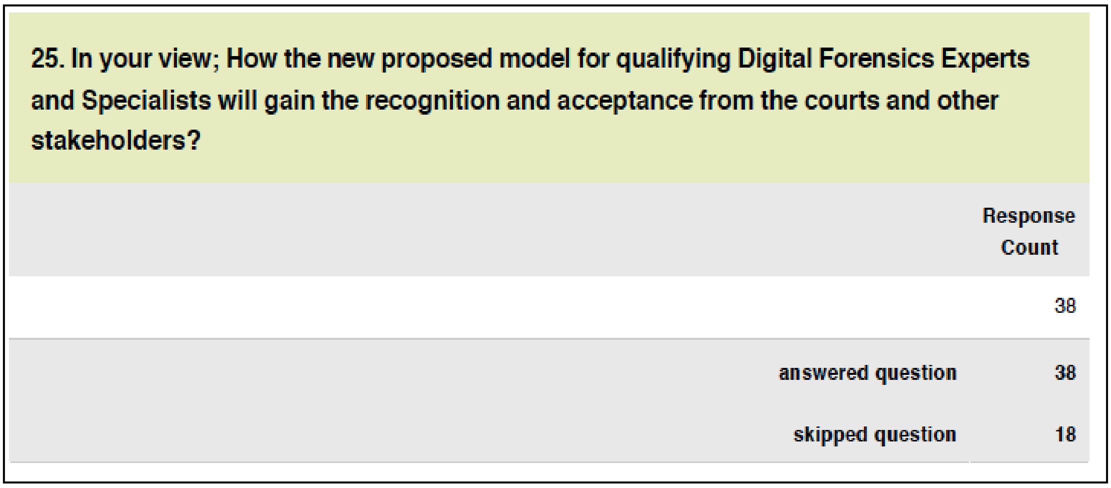
**24. Do you believe that a new proposed model will replace the existing Certification and licensing of Digital Forensics Specialists models?**

| | | Response Percent | Response Count |
|---|---|---|---|
| Yes | | 26.3% | 10 |
| No | | 34.2% | 13 |
| Not Sure | | 39.5% | 15 |
| | | Comments | 6 |
| | | answered question | 38 |
| | | skipped question | 18 |

Thirty-eight participants responded, with 26.3% positive, 34.2% negative and 39.5% answered this question not sure. This indicates a tendency to keep the current systems in place or misunderstanding of the “new model” concept, which is clear from the significant “Not sure” percentage.

Qualitative analysis of the comments revealed worries that the current certification systems are not of good standard or complete coverage of the requirements for professional performance of a Digital Forensics Specialist. However, there was a feeling that change will take time and would be complementing existing models.

Q25:



**25. In your view; How the new proposed model for qualifying Digital Forensics Experts and Specialists will gain the recognition and acceptance from the courts and other stakeholders?**

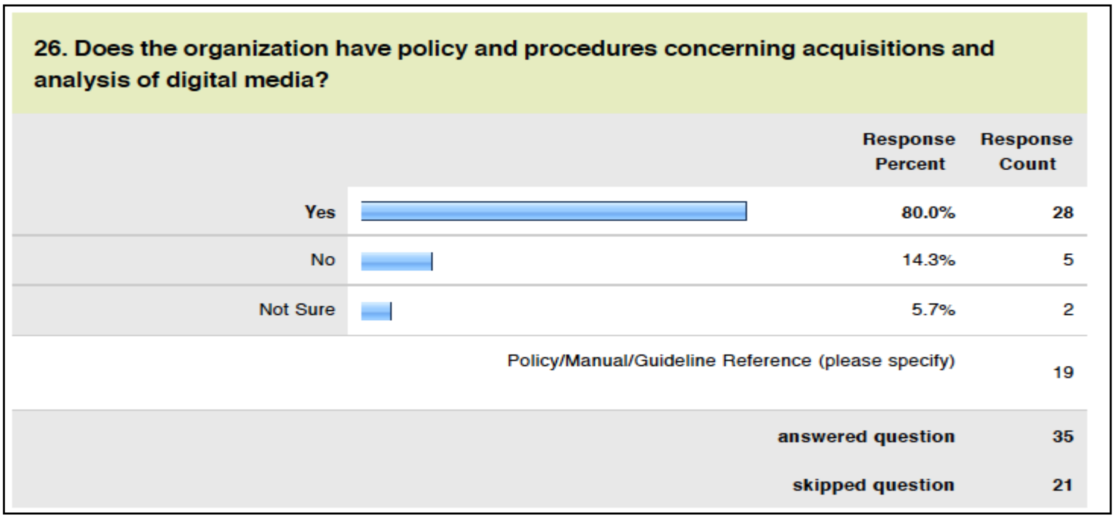
| | Response Count |
|---|---|
| | 38 |
| answered question | 38 |
| skipped question | 18 |

Qualitative analysis of the responses to this question showed a lesser confusion with standards of laboratory certification like ISO17025 however, the quest for standardizing was clear. The comments clearly expected huge recognition given quality and standards are comprehensive and outcome of licensing people on the new model demonstrate efficient and competent performance. In general, evolution overtime rather than a revolutionary jump to a new model was also seen as a natural process. There have been a couple of pessimistic comments that courts will not accept.

In summary, these were the main points proposed requirements to help recognition of a new model by the courts and other stakeholders (lawyers and firms):

- Covering international needs
- Quality of the qualification: should include process standard
- Uses Competency based testing process
- Results in demonstrated performance before courts and lawyers
- Involving courts in the establishment of the new model
- Supported by a standard monitoring and enforcing body for assessment, for example the Forensic Science regulator or the council for registration of Forensic Practitioners
- By including current successful models
- Includes experience component
- Be supported by government or driven by regulation and judicial community

Q26:



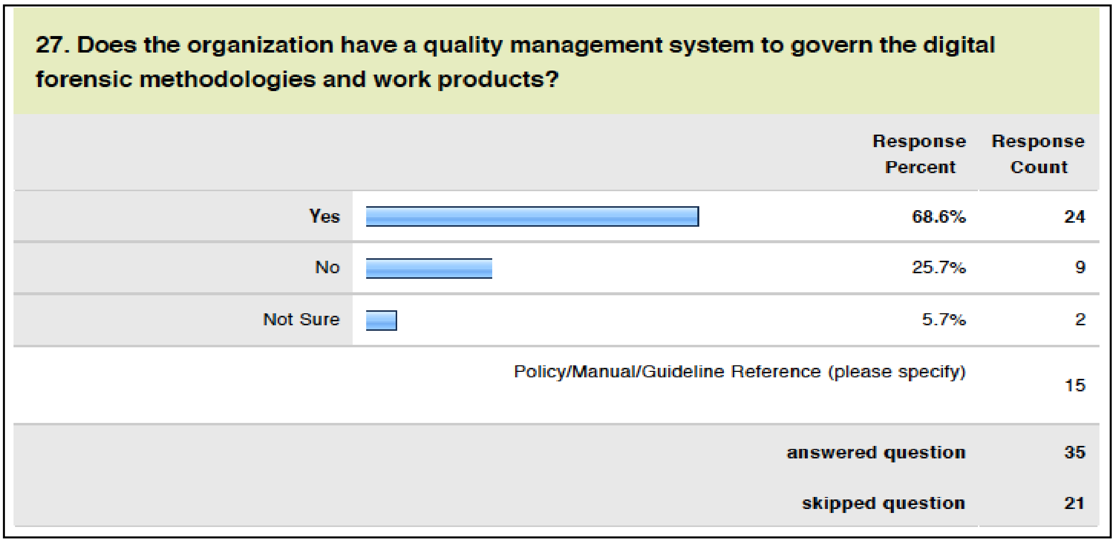
**26. Does the organization have policy and procedures concerning acquisitions and analysis of digital media?**

| | Response Percent | Response Count |
|---|---|---|
| Yes | 80.0% | 28 |
| No | 14.3% | 5 |
| Not Sure | 5.7% | 2 |
| Policy/Manual/Guideline Reference (please specify) | | 19 |
| answered question | | 35 |
| skipped question | | 21 |

Thirty-five participants responded, with 80% positive, 14.3% negative and 5.7% answered this question not sure. This indicates existing policies and procedures but does not show any uncertainty in sufficiency and adequacy of such policies as the not sure percentage is low.

Qualitative analysis of the comments revealed existence of internal policies and procedures (standard operating procedures SOPs) in compliance with such best practices and standard as: ACPO, NIST, DOj, ISO 17025, FBI manuals, etc. However, it was not clear whether the organisations are consultancy firms, or government security bodies.

Q27:



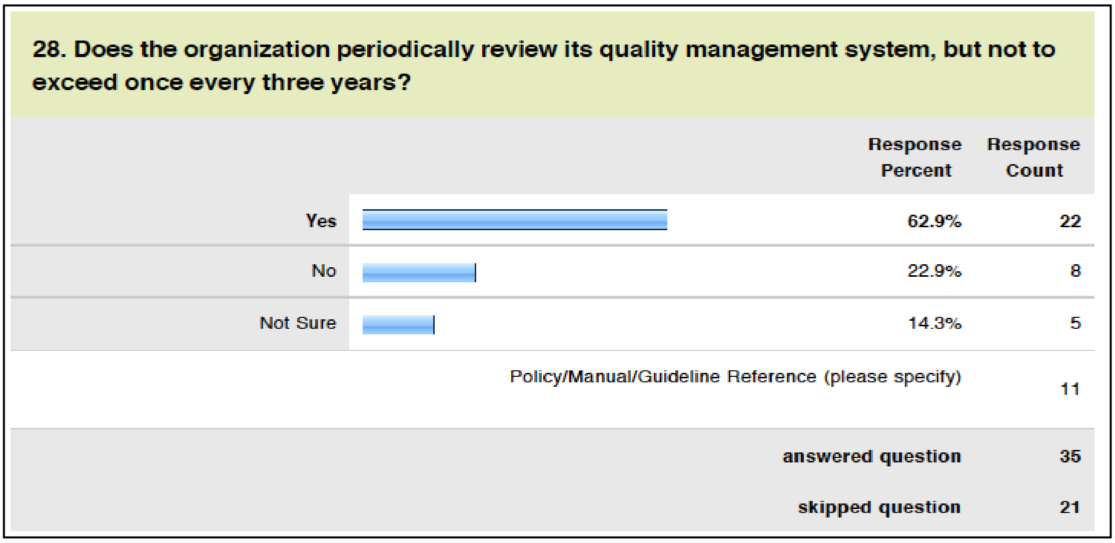
27. Does the organization have a quality management system to govern the digital forensic methodologies and work products?

| | Response Percent | Response Count |
|---|---|---|
| Yes | 68.6% | 24 |
| No | 25.7% | 9 |
| Not Sure | 5.7% | 2 |
| Policy/Manual/Guideline Reference (please specify) | | 15 |
| answered question | | 35 |
| skipped question | | 21 |

Thirty-five participants responded, with 68.8% positive, 25.7% negative and 5.7% answered this question not sure. This indicates existence of quality management systems in most organisations as viewed by participants and does not show any uncertainty in adequacy of such systems, as the not sure percentage is low.

Qualitative analysis of the comments revealed specific reliance on best practices and the one standard mentioned in the previous question and added the need for peer review and performance metrics.

Q28:



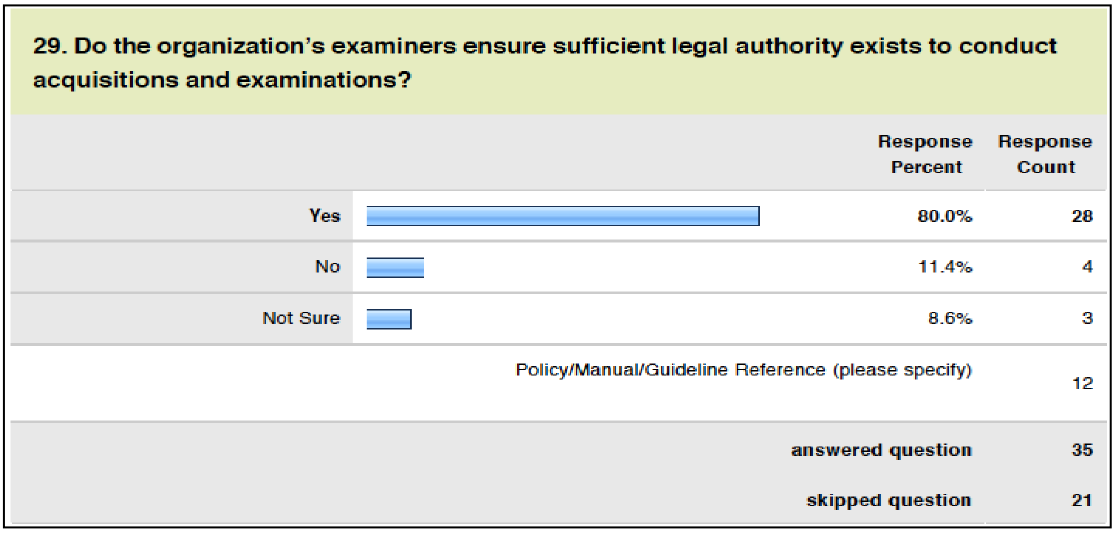
**28. Does the organization periodically review its quality management system, but not to exceed once every three years?**

| | Response Percent | Response Count |
|---|---|---|
| Yes | 62.9% | 22 |
| No | 22.9% | 8 |
| Not Sure | 14.3% | 5 |
| Policy/Manual/Guideline Reference (please specify) | | 11 |
| answered question | | 35 |
| skipped question | | 21 |

Thirty-five participants responded, with 62.9% positive, 22.9% negative and 14.3% answered this question not sure. This indicates existence of quality management systems review within 3 years in most organisations as viewed by participants.

Qualitative analysis of the comments revealed even higher frequency of review between twice annually and annually. Most reviews are based on the standard operating procedure SOPs and previously mentioned best practices.

Q29:



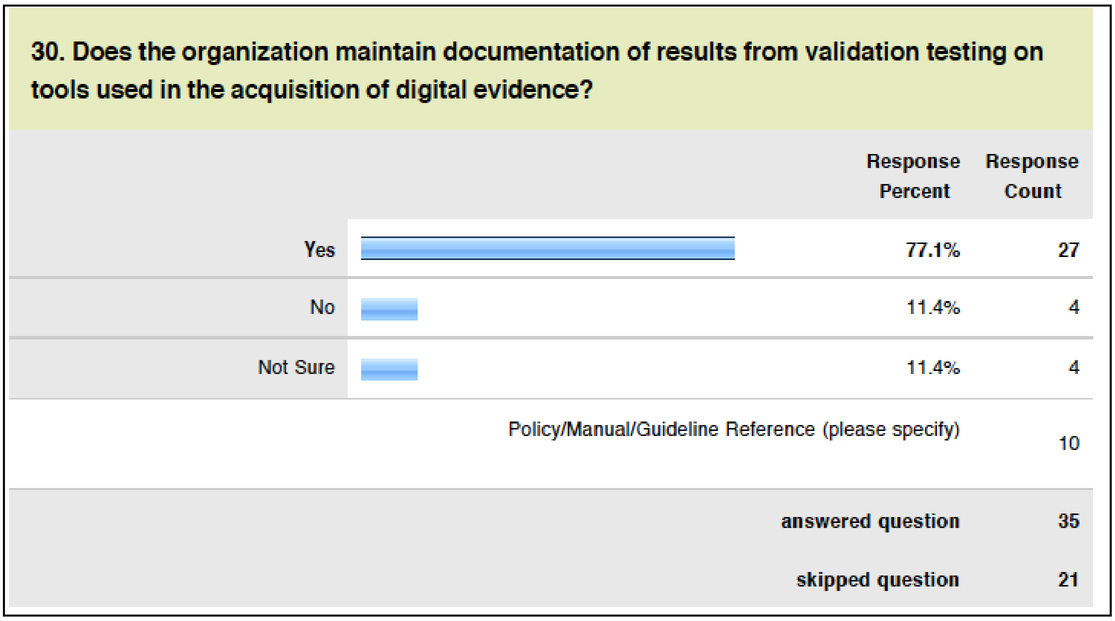
**29. Do the organization's examiners ensure sufficient legal authority exists to conduct acquisitions and examinations?**

| | Response Percent | Response Count |
|---|---|---|
| Yes | 80.0% | 28 |
| No | 11.4% | 4 |
| Not Sure | 8.6% | 3 |
| Policy/Manual/Guideline Reference (please specify) | | 12 |
| answered question | | 35 |
| skipped question | | 21 |

Thirty-five participants responded, with 80% positive, 11.4% negative and 8.6% answered this question not sure. This indicates that examiners ensure existence of legal authority to conduct acquisitions and examinations in the majority of organisations as viewed by participants.

Qualitative analysis of the comments revealed that proper documentation and search warrants are used.

<u>Q30:</u>



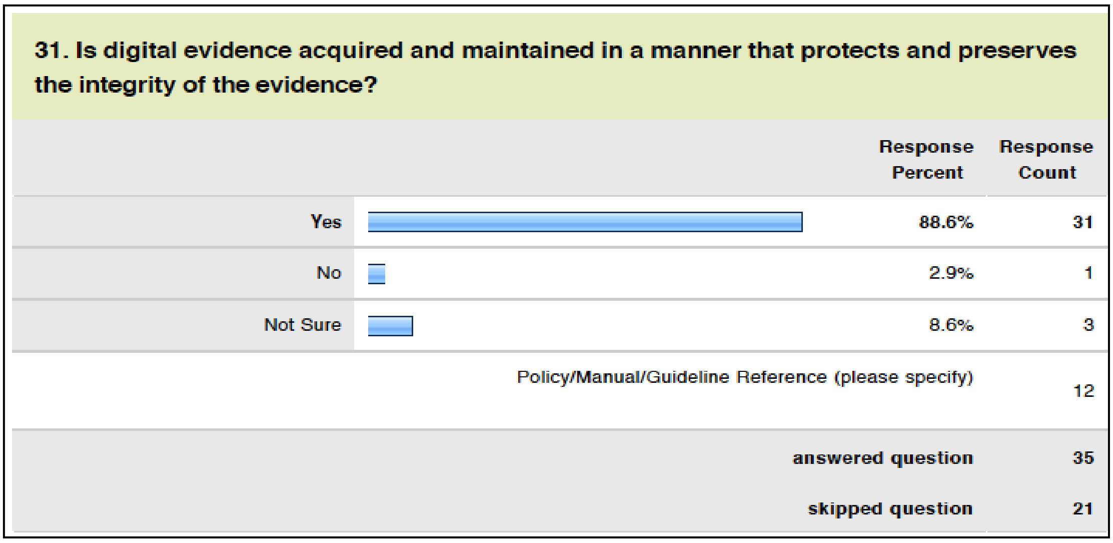
**30. Does the organization maintain documentation of results from validation testing on tools used in the acquisition of digital evidence?**

| | | Response Percent | Response Count |
|---|---|---|---|
| Yes | | 77.1% | 27 |
| No | | 11.4% | 4 |
| Not Sure | | 11.4% | 4 |
| | | Policy/Manual/Guideline Reference (please specify) | 10 |
| | | answered question | 35 |
| | | skipped question | 21 |

Thirty-five participants responded, with 77.1% positive, 11.4% negative and 11.4% answered this question not sure. This indicates existence of documentation of results from validation testing on tools used in the acquisition of digital evidence.

Qualitative analysis of the comments revealed that documentation is part of existing quality systems if any, but depends on efficiency of individuals in the organization.

Q31:



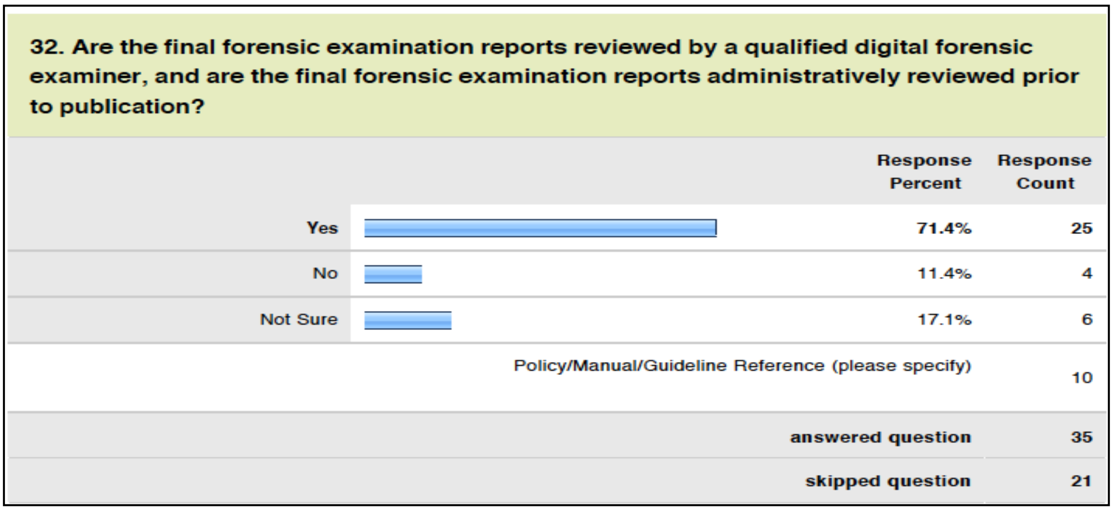
**31. Is digital evidence acquired and maintained in a manner that protects and preserves the integrity of the evidence?**

| | | Response Percent | Response Count |
|---|---|---|---|
| Yes | | 88.6% | 31 |
| No | | 2.9% | 1 |
| Not Sure | | 8.6% | 3 |
| | | Policy/Manual/Guideline Reference (please specify) | 12 |
| | | answered question | 35 |
| | | skipped question | 21 |

Thirty-five participants responded, with 88.6% positive, 2.9% negative and 8.6% answered this question not sure. This indicates proper maintenance and integrity of evidence.

Qualitative analysis of the comments revealed compliance to of APCO, ISO best practice and standards.

Q32:



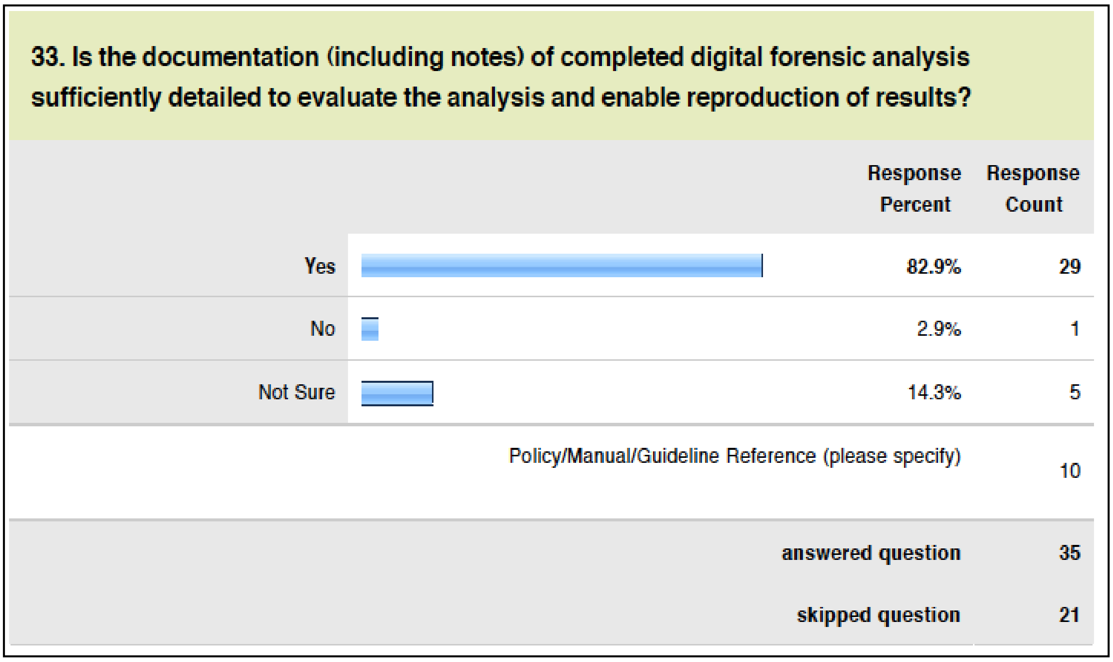
**32. Are the final forensic examination reports reviewed by a qualified digital forensic examiner, and are the final forensic examination reports administratively reviewed prior to publication?**

| | | Response Percent | Response Count |
|---|---|---|---|
| Yes | | 71.4% | 25 |
| No | | 11.4% | 4 |
| Not Sure | | 17.1% | 6 |
| | | Policy/Manual/Guideline Reference (please specify) | 10 |
| | | answered question | 35 |
| | | skipped question | 21 |

Thirty-five participants responded, with 71.4% positive, 11.4% negative and 17.1% answered this question not sure. This indicates proper handling and review of reports.

Qualitative analysis of the comments revealed compliance to lab standards and use of logs.

Q33:



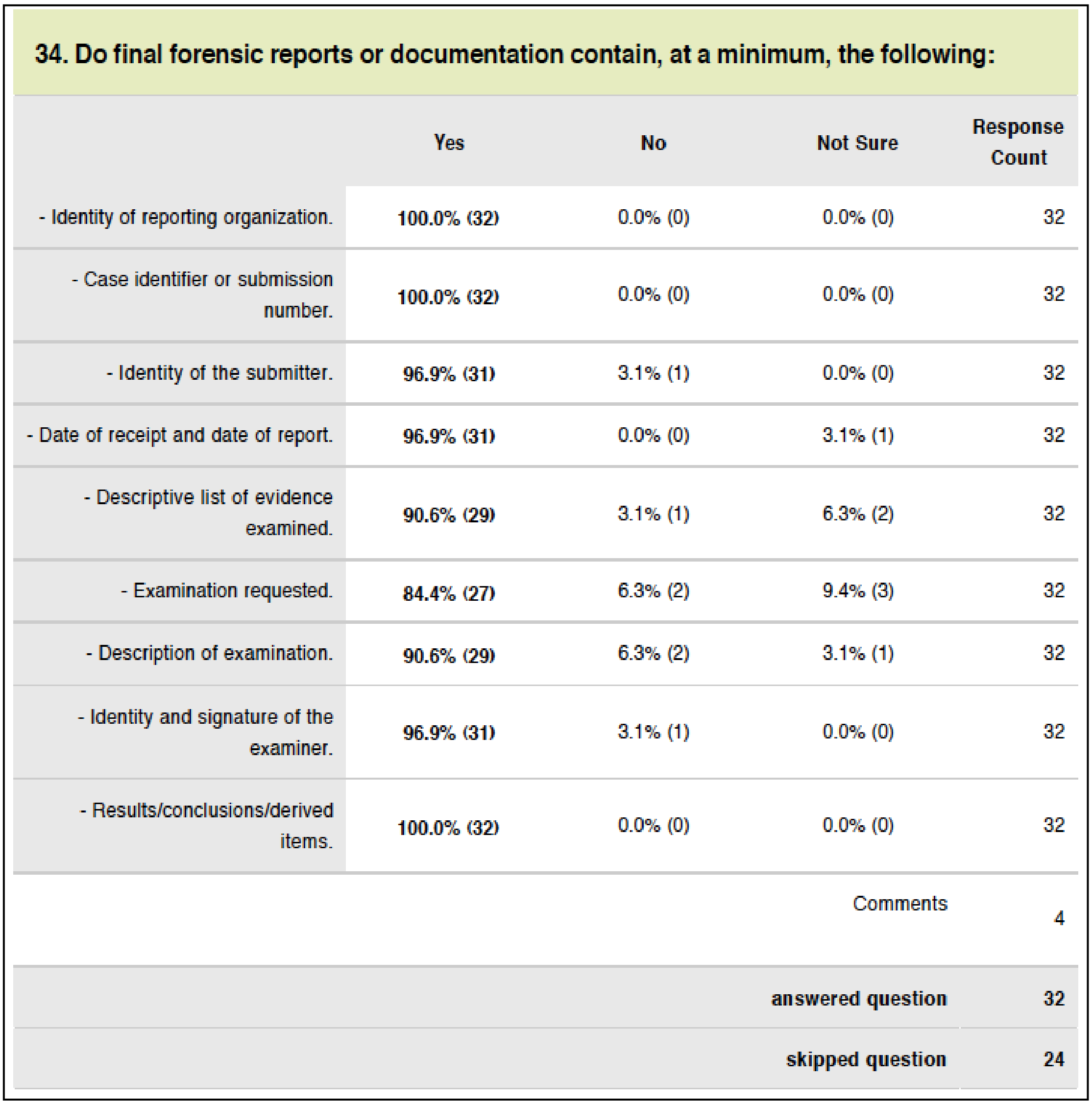
33. Is the documentation (including notes) of completed digital forensic analysis sufficiently detailed to evaluate the analysis and enable reproduction of results?

| | Response Percent | Response Count |
|---|---|---|
| Yes | 82.9% | 29 |
| No | 2.9% | 1 |
| Not Sure | 14.3% | 5 |
| Policy/Manual/Guideline Reference (please specify) | | 10 |
| answered question | | 35 |
| skipped question | | 21 |

Thirty-five participants responded, with 82.9% positive, 2.9% negative and 14.3% answered this question not sure. This indicates that the majority have sufficient analysis documentation to enable proper evaluation and reproduction of results.

Qualitative analysis of the comments revealed majority compliance to policy, ISO17025 standards.

Q34:



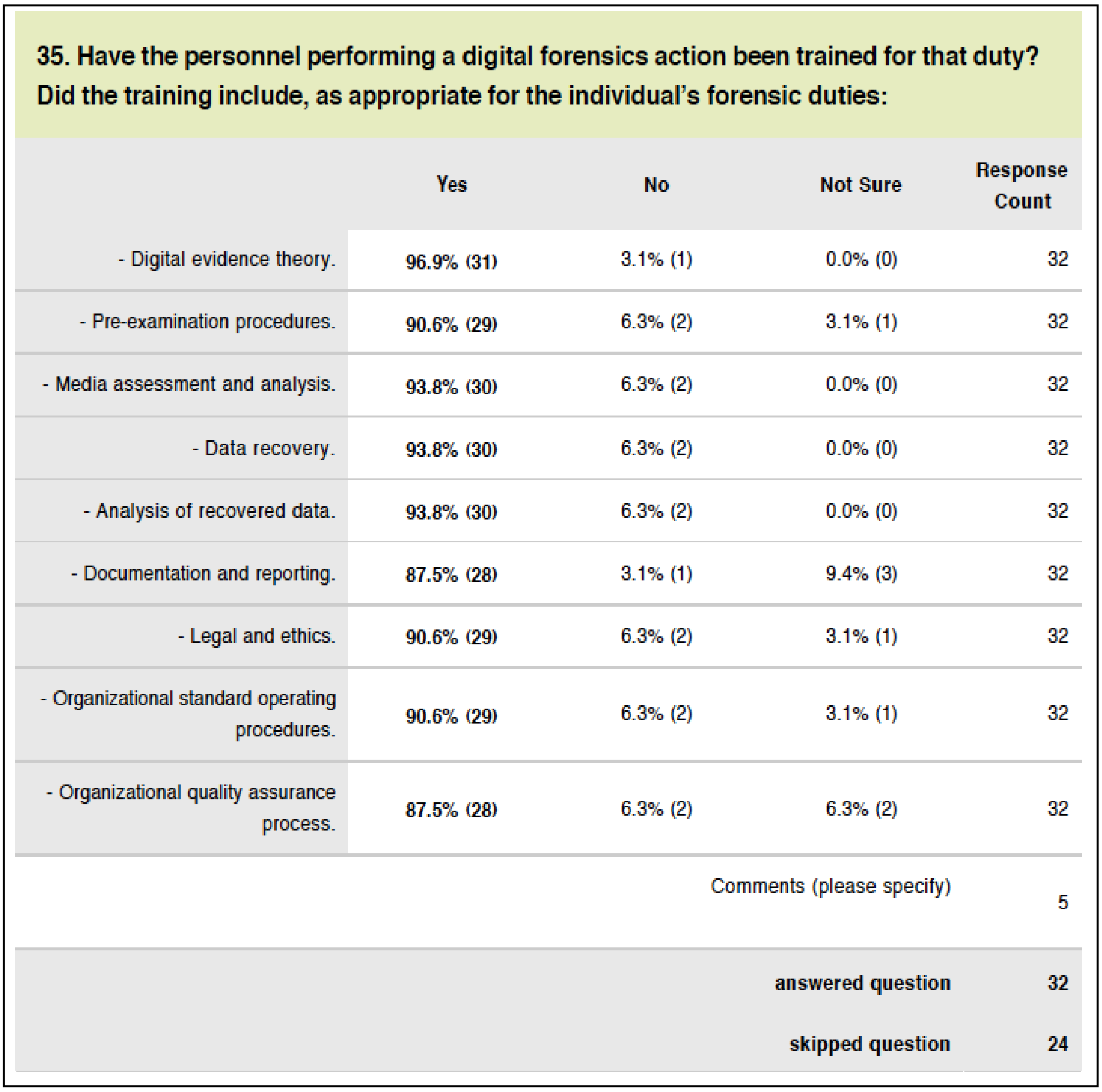
**34. Do final forensic reports or documentation contain, at a minimum, the following:**

| | Yes | No | Not Sure | Response Count |
|---|---|---|---|---|
| - Identity of reporting organization. | 100.0% (32) | 0.0% (0) | 0.0% (0) | 32 |
| - Case identifier or submission number. | 100.0% (32) | 0.0% (0) | 0.0% (0) | 32 |
| - Identity of the submitter. | 96.9% (31) | 3.1% (1) | 0.0% (0) | 32 |
| - Date of receipt and date of report. | 96.9% (31) | 0.0% (0) | 3.1% (1) | 32 |
| - Descriptive list of evidence examined. | 90.6% (29) | 3.1% (1) | 6.3% (2) | 32 |
| - Examination requested. | 84.4% (27) | 6.3% (2) | 9.4% (3) | 32 |
| - Description of examination. | 90.6% (29) | 6.3% (2) | 3.1% (1) | 32 |
| - Identity and signature of the examiner. | 96.9% (31) | 3.1% (1) | 0.0% (0) | 32 |
| - Results/conclusions/derived items. | 100.0% (32) | 0.0% (0) | 0.0% (0) | 32 |
| | | | Comments | 4 |
| | | | **answered question** | **32** |
| | | | **skipped question** | **24** |

Thirty-two participants responded, with above 84.4% positive, max of 6.3% negative and a max of 9.4%, answered this question not sure. This indicates that the majority of participants practice the listed documentation criteria.

Qualitative analysis of the comments revealed that there is very little confusion in this area.

Q35:



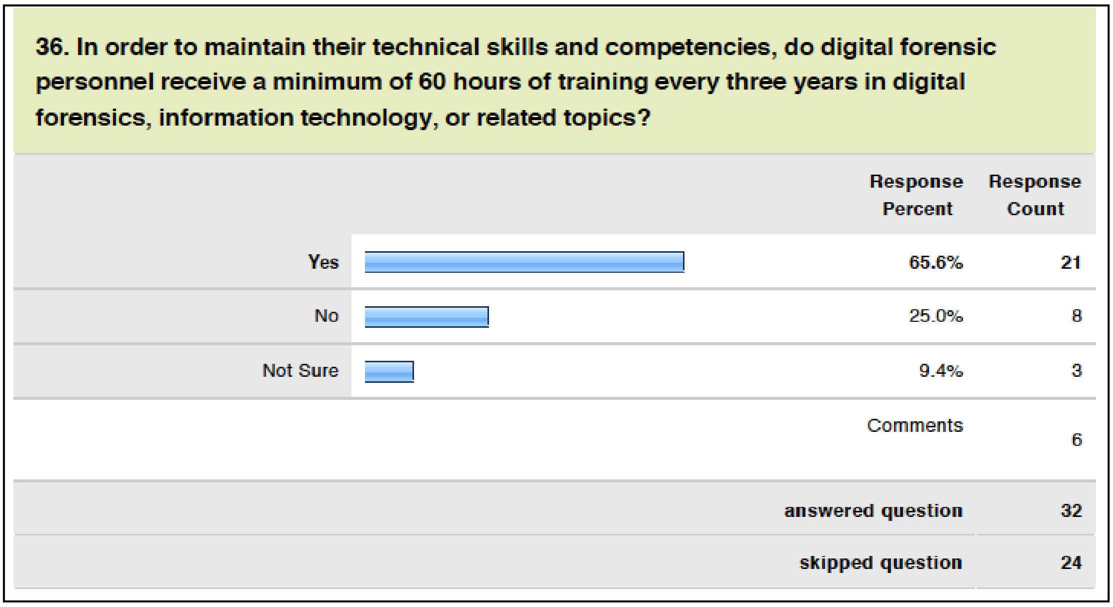
**35. Have the personnel performing a digital forensics action been trained for that duty? Did the training include, as appropriate for the individual's forensic duties:**

| | Yes | No | Not Sure | Response Count |
|---|---|---|---|---|
| - Digital evidence theory. | 96.9% (31) | 3.1% (1) | 0.0% (0) | 32 |
| - Pre-examination procedures. | 90.6% (29) | 6.3% (2) | 3.1% (1) | 32 |
| - Media assessment and analysis. | 93.8% (30) | 6.3% (2) | 0.0% (0) | 32 |
| - Data recovery. | 93.8% (30) | 6.3% (2) | 0.0% (0) | 32 |
| - Analysis of recovered data. | 93.8% (30) | 6.3% (2) | 0.0% (0) | 32 |
| - Documentation and reporting. | 87.5% (28) | 3.1% (1) | 9.4% (3) | 32 |
| - Legal and ethics. | 90.6% (29) | 6.3% (2) | 3.1% (1) | 32 |
| - Organizational standard operating procedures. | 90.6% (29) | 6.3% (2) | 3.1% (1) | 32 |
| - Organizational quality assurance process. | 87.5% (28) | 6.3% (2) | 6.3% (2) | 32 |
| | | | Comments (please specify) | 5 |
| | | | **answered question** | **32** |
| | | | **skipped question** | **24** |

Thirty-two participants responded, with above 87 % positive, max of 6.4% negative and a max of 9.4%, answered this question not sure. This indicates that training of participants exists by large and follows the listed criteria.

Qualitative analysis of the comments revealed existing certification in this area but not all have taken certification.

Q36:



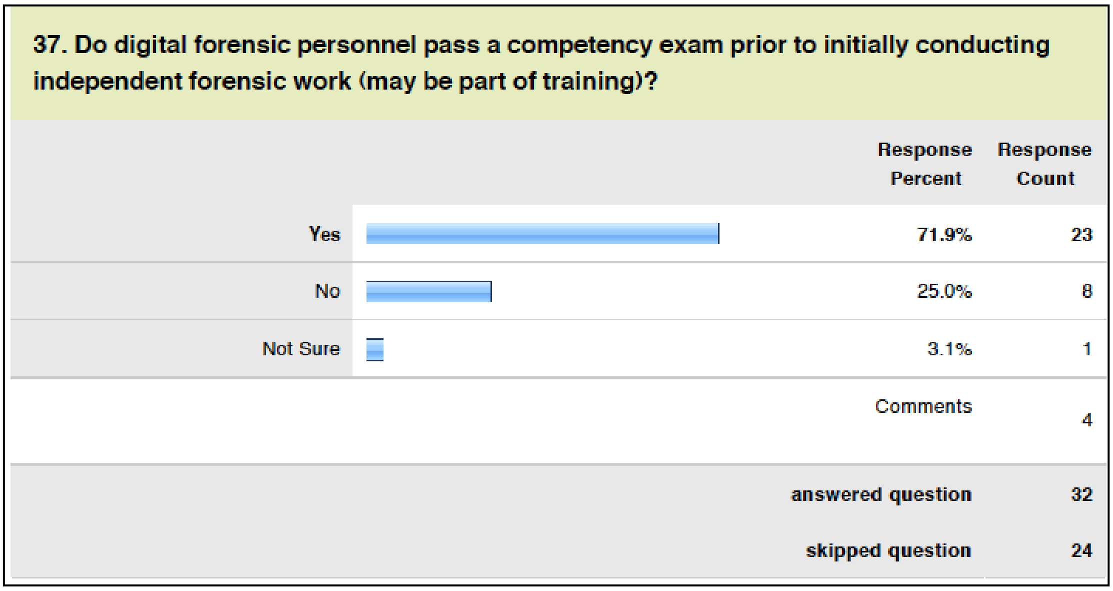
**36. In order to maintain their technical skills and competencies, do digital forensic personnel receive a minimum of 60 hours of training every three years in digital forensics, information technology, or related topics?**

| | Response Percent | Response Count |
|---|---|---|
| Yes | 65.6% | 21 |
| No | 25.0% | 8 |
| Not Sure | 9.4% | 3 |
| | Comments | 6 |
| | answered question | 32 |
| | skipped question | 24 |

Thirty-two participants responded, with 65.6 % positive, 25.0% negative and 9.4% answered this question not sure. This indicates that the majority of participants receive the listed training.

Qualitative analysis of the comments revealed that even more than 60 hours of training is taken for the majority however budget limitation hampers some participants from the right training.

Q37:



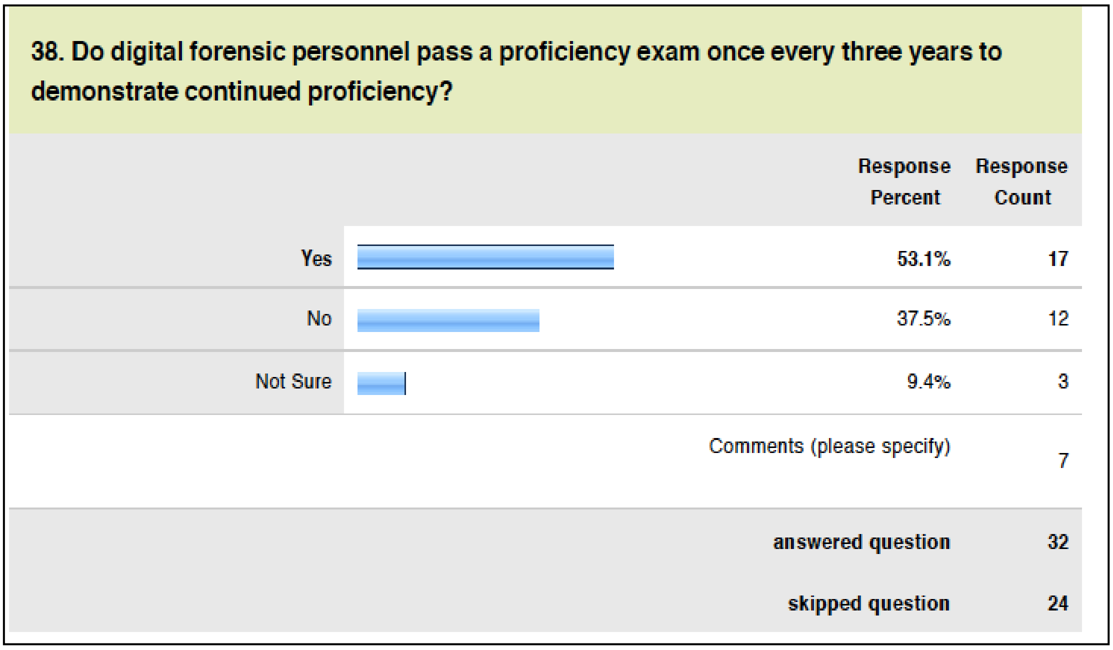
**37. Do digital forensic personnel pass a competency exam prior to initially conducting independent forensic work (may be part of training)?**

| | Response Percent | Response Count |
|---|---|---|
| Yes | 71.9% | 23 |
| No | 25.0% | 8 |
| Not Sure | 3.1% | 1 |
| | Comments | 4 |
| | answered question | 32 |
| | skipped question | 24 |

Thirty-two participants responded, with 71.9 % positive, 25.0% negative and 3.1% answered this question not sure. This indicates that the majority of participants pass competency tests.

Qualitative analysis of the comments revealed that there is varying opinion and practices left to practice and authorized personnel to decide. However, APCO and EnCE do not include a complying request for such exams.

Q38:



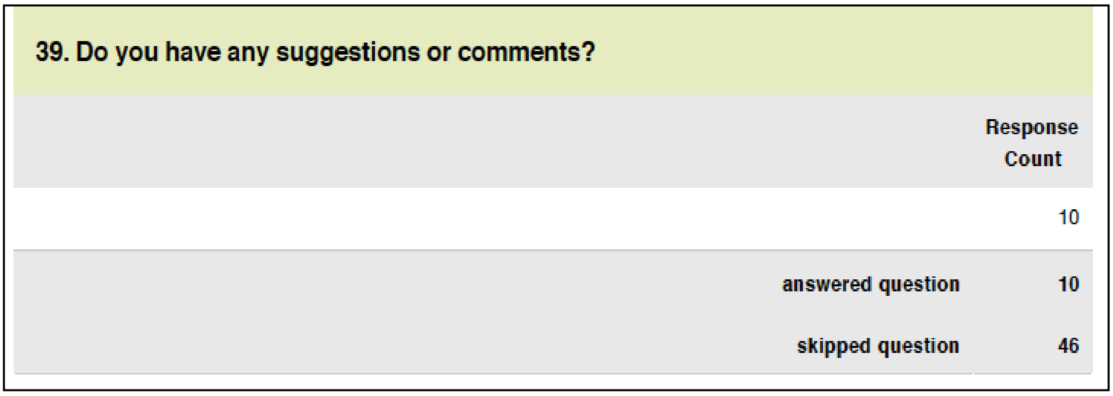
38. Do digital forensic personnel pass a proficiency exam once every three years to demonstrate continued proficiency?

| | Response Percent | Response Count |
|---|---|---|
| Yes | 53.1% | 17 |
| No | 37.5% | 12 |
| Not Sure | 9.4% | 3 |
| | Comments (please specify) | 7 |
| | answered question | 32 |
| | skipped question | 24 |

Thirty-two participants responded, with 53.1 % positive, 37.5% negative and f 9.4% answered this question not sure. This indicates that the majority of participants pass exams but a significant part of the sample does not.

Qualitative analysis of the comments revealed that such exam frequency is part of ACE and ENCE processes and that some just maintain CPD points. There has been an indication of fear of failure in such exams and cost involved which was reflected in comments and in the quantitative results.

Q39:



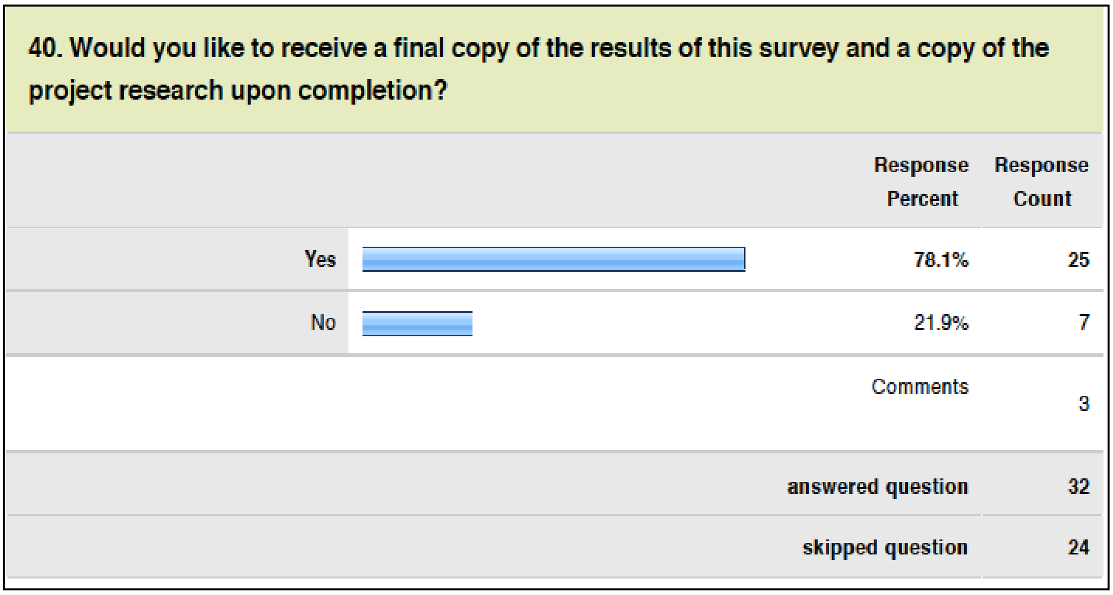
39. Do you have any suggestions or comments?

| | Response Count |
|---|---|
| | 10 |
| answered question | 10 |
| skipped question | 46 |

Ten participants responded to this question and the suggestions can be summarised as:

- Interest in the Model project
- The need for a comprehensive model is important
- Once a model is in place the European Union must regulate enforcing it
- Budget may be a challenge
- There is a dilemma of variation of legislation and practices in different countries.

Q40:



40. Would you like to receive a final copy of the results of this survey and a copy of the project research upon completion?

| | | Response Percent | Response Count |
|---|---|---|---|
| Yes | | 78.1% | 25 |
| No | | 21.9% | 7 |
| | | Comments | 3 |
| | | answered question | 32 |
| | | skipped question | 24 |

Thirty-two participants responded to this question and 78.1% showed interest in sharing results of the survey, which indicate interest in this project among more than half of the original participants.

# APPENDIX D: EXTRACT OF INTERVIEW – LAB CHALLENGES

**(LAB_A_Interviews, 2012)**… Increasingly law enforcement digital forensic labs are being swamped with standards related and regulatory requirements. The task of simply understanding them, implementing them, integrating them and measuring the effectiveness of them is proving to be a goliath task, and we are continuously behind the curve. Instead of focussing on present day challenges and long-term research and development related to our field, we are forced to now become regulatory, ISO, and business process re-engineering practitioners, using out-dated, ill-suited traditional business methods and philosophies. We need a solution designed specifically for Digital Forensics, which caters not just for our technical needs, but those needs being forced upon us by our parent organisations. Criminal syndicates work together, share their best practices, and help find ways to make their businesses more efficient, we could learn a thing or two about cooperation and more effective and timely knowledge sharing with them. Efficiency and capability ratings in many digital forensic labs today are based upon misleading so-called measures of efficiency adopted from conventional policing such as:

- Number of cases received
- Number of devices examined
- Source of case referrals

None of which gives any bearing as to how efficient we are, our challenges and areas for improvement. We end up having to run multiple tracking systems, to track statistics that really have no bearing on how well we are doing as required by our organisation, and a separate system of things that really matter to us, such as Service Levels, Customer satisfaction, but have no means to measure or manage our capability maturity”.

# APPENDIX E: SAMPLE OF ASSESSMENT TOOL WORKSHEETS

## DF-C²M² Assessment Ratings – LAB #1: Service Catalogue – Digital Audio & Video:

| Category | Service Description | Service Delivery Group | Dependency on Other Service Identified | Status | % Implemented | Core or Value Add? |
|---|---|---|---|---|---|---|
| DA&VF1 | Digital Data Extraction from Digital Media Capture Devices | DA&V Forensics | Yes | Fully Implemented | 100 | Core |
| DA&VF2 | Digital Forensic Examination and Analysis of Digital Video | DA&V Forensics | n/a | Fully Implemented | 100 | Core |
| DA&VF3 | Digital Forensic Examination and Analysis of Digital Audio | DA&V Forensics | n/a | Fully Implemented | 100 | Core |
| DA&VF4 | Digital Forensic Examination and Analysis of Digital Images (Pictures) | DA&V Forensics | Yes | Fully Implemented | 100 | Core |
| DA&VF5 | Data Recovery from Digital Media Capture Devices | DA&V Forensics | Yes | Fully Implemented | 100 | Core |
| DA&VF6 | Digital Video Enhancement | DA&V Forensics | Yes | Fully Implemented | 100 | Core |
| DA&VF7 | Digital Image (Picture) Enhancement | DA&V Forensics | Yes | Fully Implemented | 100 | Core |
| DA&VF8 | Digital Audio Enhancement | DA&V Forensics | Yes | Fully Implemented | 100 | Core |
| DA&VF9 | Digital Audio & Video Expert Witness Testimony | DA&V Forensics | Yes | Mostly Implemented | 70 | Value Add |
| DA&VF10 | Digital Image Matching (CP Hash Database) | DA&V Forensics | Yes | Planned | 30 | Value Add |
| DA&VF11 | CD and DVD Validation and Recovery | DA&V Forensics | Yes | Planned | 30 | Value Add |

**DF-C²M² Assessment Ratings LAB #1: Service Catalogue – Cybercrime Analysis:**

| Category | Service Description | Service Delivery Group | Dependency on Other Service | Status | % Implemented | Core or Value Add? |
|---|---|---|---|---|---|---|
| CIS1 | Cyber Crime Analysis Planning | CyberCrime Examiner | n/a | Partially Implemented | 50 | Value Add |
| CIS2 | Cyber Crime Analysis Technical Support | CyberCrime Examiner | Yes | Partially Implemented | 60 | Core |
| CIS3 | Cyber Crime Analysis Tactical Support | CyberCrime Examiner | Yes | Partially Implemented | 60 | Core |
| CIS4 | Cyber Crime Analysis Evidence Acquisition | CyberCrime Examiner | Yes | Partially Implemented | 70 | Core |
| CIS5 | Cyber Crime Expert Witness Testimony | CyberCrime Examiner | Yes | Partially Implemented | 50 | Value Add |
| CIS6 | Cyber Crime Evidence Examination | CyberCrime Examiner | Yes | Partially Implemented | 50 | Core |
| CIS7 | Cyber Crime Alerts & Advisory Services | CyberCrime Examiner | Yes | Planned | 5 | Value Add |

**DF-C²M² Assessment Ratings LAB #1: Service Catalogue – Digital Evidence Tactical Support:**

| Category | Service Description | Service Delivery Group | Dependency on Other Service/ Identified | Status | % Implemented | Core Or Value Add? |
|---|---|---|---|---|---|---|
| DETS1 | Digital Evidence Tactical Support & Advice | DFL Team | Yes | Partially Implemented | 50 | Core |
| DETS2 | Digital Evidence Handling and Seizure Training | DFL Team | Yes | Partially Implemented | 50 | Core |
| DETS3 | Digital Forensics Advisory Services | DFL Team | Yes | Partially Implemented | 50 | Value Add |
| DETS4 | Cyber Crime & Digital Forensics Awareness (Outreach) | DFL Team | Yes | Partially Implemented | 50 | Value Add |
| DETS5 | Digital Forensics Training | DFL Team | Yes | Partially Implemented | 50 | Value Add |

**Service Catalogue – Network & Live Forensics:**

| Category | Service Description | Service Delivery Group | Dependency on Other Service | Status | % Implemented | Core Or Value Add? |
|---|---|---|---|---|---|---|
| NF1 | Live & Network Forensics On Site Evidence Capture | Net Forensics | All CF Services | Partially Implemented | 50 | Core |
| NF2 | Live & Network Forensics Data Examination & Analysis | Net Forensics | CF1, CF2, CF3, CF4, NF1 | Partially Implemented | 50 | Core |
| NF3 | Live & Network Forensics Tactical Support On Site | Net Forensics | NF2 | Partially Implemented | 50 | Value Add |

**Service Catalogue – Health, Safety & Security:**

| Category | Description | Score | | |
|---|---|---|---|---|
| | | Level | Rating | Required |
| **HS** | **Health, Safety & Security** | | | |
| HS1 | Accesses to lab facilities are restricted and all visitor access is logged in the Visitor access log book. | Level 3 – Full Deployment | **3** | **5** |
| HS2 | Lab personnel are trained on Health & Safety requirements such as use of protective garments (gloves, etc.), what to do in event of fir as defined within Health, Safety &Security, e Procedures (Manual). | Level 5 - Continuously Improving | **5** | **5** |
| HS3 | Lab has designated First Aid office trained and certified in First Aid & CPR (and a deputy). | Level 3 – Full Deployment | **4** | **5** |
| HS4 | Lab has fire detection and suppression system covering all areas especially evidence storage). | Level 1 - Documented | **1** | **5** |
| HS5 | Lab has access control and physical key access for key areas of lab. | Level 3 – Full Deployment | **3** | **5** |
| HS6 | Lab access and movement is recorded on CCTV for a defined minimum retention period as per legal requirement/Organisational policy. | Level 3 – Full Deployment | **3** | **5** |
| HS7 | Lab is monitored by an Intruder detection/alarm system 24/7. | Level 1 – Documented | **1** | **5** |
| HS8 | All personnel granted access to Lab signed a Lab Access/Authorizations document that details their responsibilities regarding lab access. | Level 3 – Full Deployment | **3** | **5** |
| HS9 | Lab access is revoked for personnel no longer employed by the lab, and suspended during vacations via electronic access control system. | Level 3 – Full Deployment | **3** | **5** |
| HS10 | Lab has a disaster recovery plan in place that is tested at least annually. | Level 1 – Documented | **1** | **5** |
| HS11 | Lab ensures that case data is secured stored and access is restricted and audited. | Level 3 – Full Deployment | **3** | **5** |
| HS12 | Lab has well-defined information security requirements for all case data and storage of electronic evidence of lab servers/SANS and removable media (CDs/DVDs). | Level 3 – Full Deployment | **3** | **5** |
| HS13 | Lab operational network is physically separate for any other networks within the Organisation and the Internet. | Level 4 - Measured & Automated | **4** | **5** |

| | | | | |
|---|---|---|---|---|
| HS14 | The use of removable media within the lab is regulated and controlled. | Level 3 – Full Deployment | **3** | **5** |
| HS15 | Destruction requirements of any printed matter (forms, etc.) if defined within H&S procedures. | Level 3 – Full Deployment | **3** | **5** |
| HS16 | Destruction of any electronic data is defined with Information Security policies and procedures. | Level 3 – Full Deployment | **3** | **5** |
| HS17 | The permitted use of encryption to restrict access to certain data is tightly controlled and requirements clearly defined within Lab policies. | Level 3 – Full Deployment | **3** | **5** |
| HS18 | Media used to source evidence/images for source devices is first wiped and then verified using equipment designed specifically for that purpose. | Level 4 - Measured & Automated | **4** | **5** |
| HS19 | Lab has a well-defined policy for dealing with any media that may potentially have been exposed or be contaminated by Biological and chemical hazards. | Level 4 - Measured & Automated | **4** | **5** |
| HS20 | Lab Fire and security equipment is serviced and tested at least every 6 months. | Level 4 - Measured & Automated | **4** | **5** |
| HS21 | Lab trains all personnel of use of Anti-Static precautions. | Level 4 - Measured & Automated | **4** | **5** |
| HS22 | Lab is able to continue operations/processing of data without damage to any devices/evidence in the event of a power outage. | Level 3 – Full Deployment | **3** | **5** |
| HS23 | Lab personnel sign a Lab-specific Non-Disclosure agreement (in their individual capacity) as part of their Code of Conduct agreement upon joining the lab, and this is renewed every two years. | Level 3 – Full Deployment | **3** | **5** |
| HS24 | Lab has a case classification system that details need to know requirements of certain types of cases, including how to store, protect and transmit sensitive information e.g.: related to Illicit images (as per legal requirements). | Level 2– Partial Deployment | **2** | **5** |
| HS25 | Lab has well-defined service and maintenance plan for all equipment used in extraction/examination of evidence. | Level 3 – Full Deployment | **3** | **5** |
| HS26 | Lab has designated Information Security Officer role defined and assigned to an individual. | Level 1 - Documented | **1** | **5** |
| | **Total Score** | | **77** | **130** |
| | **Maturity Level Average** | **Level 3 – Full Deployment** | **2.99** | |

**Operations – LAB #1:**

| Category | Description | Score | | |
|---|---|---|---|---|
| | | Level | Rating | Required |
| **OP** | **Operations** | | | |
| OP1 | Lab has well-defined case acceptance and rejection processes and criteria. | Level 4 - Measured & Automated | 4 | 5 |
| OP2 | Lab has well-defined procedures that deal with requests that go beyond current lab capabilities including the use of sub-contracting to other labs (if permitted). | Level 4 - Measured & Automated | 4 | 5 |
| OP3 | Lab has well-defined evidence handling a chain of custody processes. | Level 5 - Continuously Improving | 5 | 5 |
| OP4 | Lab has well-defined case management process to accept, assign, track and provide status updates to customers of cases. | Level 3 - Full Deployment | 3 | 5 |
| OP5 | Lab has well-defined evidence and exhibit labelling, marking and tracking system. | Level 3 - Full Deployment | 3 | 5 |
| OP6 | Lab has procedures to track use of media including re-supply/re-order of consumables. | Level 5 - Continuously Improving | 5 | 5 |
| OP7 | Lab has system in place to track equipment/license warranties, maintenance and renewals. | Level 5 - Continuously Improving | 5 | 5 |
| OP8 | Lab tests all equipment received before commissioning. | Level 4 - Measured & Automated | 4 | 5 |
| OP9 | Lab has defined test data sets, and procedures for testing and verifying equipment and tools before start of each case. | Level 4 - Measured & Automated | 4 | 5 |
| OP10 | Lab has system for measuring and implement overall process improvement across all areas of lab processes (e.g.: CMM model, Six Sigma or similar). | Level 3 - Full Deployment | 3 | 5 |
| OP11 | Lab has defined procedures for tool validation and approval. | Level 3 - Full Deployment | 3 | 5 |
| | **Total Score** | | **43** | **55** |
| | **Maturity Level Average** | **Level 3 - Full Deployment** | **3.91** | |

**Audit – LAB #1:**

| Category | Description | Score | | |
|---|---|---|---|---|
| | | Level | Rating | Required |
| **A** | **Audit** | | | |
| A1 | Technical peer review of examination process, analysis and findings conducted for each case. | Level 5 - Continuously Improving | **5** | **5** |
| A2 | Administrative peer review of process compliance is conducted for each case. | Level 4 - Measured & Automated | **4** | **5** |
| A3 | Case report reviewed and explained to the customer. | Level 2 - Partial Deployment | **2** | **5** |
| A4 | Customer feedback of examination timeliness, report, to be solicited and documented upon completion of each case. | Level 4 - Measured & Automated | **4** | **5** |
| A5 | Each new case type (e.g.: new device) should be treated as a lessons learnt opportunity and new knowledge gained related to tools or processes shared with other examiners via Knowledge base. | Level 2 - Partial Deployment | **2** | **5** |
| A6 | Any areas of improvement or shortcomings should be identified and addressed via Corrective/Preventative Actions. | Level 4 - Measured & Automated | **4** | **5** |
| | **Total Score** | | **21** | **30** |
| | **Maturity Level Average** | **Level 3 - Full Deployment** | **3.5** | |

**Assessor's Comment:**

Sound practical systems and policies in place in line with quality standards and accepted best practices and legal requirements.

**Quality Best Practices LAB #1:**

| Category | Description | Score | | |
|---|---|---|---|---|
| | | Level | Rating | Required |
| QBP | Quality Best Practices | | | |
| QBP1 | Internal Quality Management System | Level 4 - Measured & Automated | 4 | 5 |
| QBP2 | ISO 17025 | Level 4 - Measured & Automated | 4 | 5 |
| QBP3 | Peer Review and Internal Audit process | Level 4 - Measured & Automated | 4 | 5 |
| QBP4 | Handling Digital Evidence (H&S) | Level 3 - Full Deployment | 3 | 5 |
| QBP5 | First Aid Guidelines | Level 3 - Full Deployment | 3 | 5 |
| | **Total Score** | | **18** | **25** |
| | **Maturity Level Average** | **Level 3 - Full Deployment** | **3.60** | |

Assessor’s Comment:

Sound practical systems and policies in place in line with quality standards and accepted best practices and legal requirements, fully implemented and regularly revised and updated.

## General Best Practices:

| Category | Description | Score | | |
|---|---|---|---|---|
| | | Level | Rating | Required |
| **GPB** | **General Best Practices** | | | |
| GPB1 | Lab Policies encourage and promote the development, use and sharing of best practices. | Level 2 - Partial Deployment | **2** | **5** |
| GPB2 | Lab uses industry accepted best practices for all technical and evidence handling aspects. | Level 4 - Measured & Automated | **4** | **5** |
| GPB3 | Lab methods for tools and process are based on an reference industry accepted best practices. | Level 4 - Measured & Automated | **4** | **5** |
| GPB4 | Lab publishes selected internal best practices for peer review at least twice per annum. | Level 4 - Measured & Automated | **4** | **5** |
| GPB5 | External Best practices references are revised and updated as may be required and are referenced. | Level 4 - Measured & Automated | **4** | **5** |
| GPB6 | Best practices used for Imaging. | Level 4 - Measured & Automated | **4** | **5** |
| GPB7 | Best Practices used for Computer Examination with Encase. | Level 4 - Measured & Automated | **4** | **5** |
| GPB8 | Best Practices used for Computer Examination with FTK. | Level 4 - Measured & Automated | **4** | **5** |
| GPB9 | Best Practices used for Computer Examination with Xways. | Level 4 - Measured & Automated | **4** | **5** |
| GPB10 | Best Practices used for Mobile Examination with XRY. | Level 4 - Measured & Automated | **4** | **5** |
| GPB11 | Best Practices used for Mobile Examination with UFED. | Level 4 - Measured & Automated | **4** | **5** |
| GPB12 | Best Practices used for Media Wiping & verification. | Level 4 - Measured & Automated | **4** | **5** |
| GPB13 | Best Practices used for Workstation verification & testing. | Level 4 - Measured & Automated | **4** | **5** |
| GPB14 | Best Practices used for Tool validation and testing. | Level 4 - Measured & Automated | **4** | **5** |
| GPB15 | Best Practices used for Evidence Storage and Chain Of Custody handling. | Level 4 - Measured & Automated | **4** | **5** |
| GPB16 | Best Practices used for Evidence Storage. | Level 4 - Measured & Automated | **4** | **5** |
| GPB17 | Best Practices used for Authorized Data Destruction. | Level 4 - Measured & Automated | **4** | **5** |

| | | | | |
|---|---|---|---|---|
| GPB18 | Best Practices used for Information Security Controls. | Level 2 – Partial Deployment | **2** | **5** |
| GPB19 | Best Practices used for Digital Video Extraction. | Level 4 - Measured & Automated | **4** | **5** |
| GPB20 | Best Practices used for Digital Video Clarification. | Level 4 - Measured & Automated | **4** | **5** |
| GPB21 | Best Practices used for Digital Evidence Reporting. | Level 4 - Measured & Automated | **4** | **5** |
| GPB22 | Best Practices used for Technical Peer Review. | Level 4 - Measured & Automated | **4** | **5** |
| GPB23 | Best Practices used for Case Audits. | Level 4 - Measured & Automated | **4** | **5** |
| GPB24 | Defined procedure for creation, review and approval of internal best practices. | Level 4 - Measured & Automated | **4** | **5** |
| GPB25 | Defined procedure for publishing/sharing of internal best practices with external parties. | Level 4 - Measured & Automated | **4** | **5** |
| GPB26 | Best Practices used for Volatile Data Acquisition & Analysis. | Level 4 - Measured & Automated | **4** | **5** |
| GPB27 | Best Practices used for Online Data Acquisition & Analysis. | Level 4 - Measured & Automated | **4** | **5** |
| **Total Score** | | | **83** | **135** |
| **Maturity Level Average** | | **Level 3 – Full Deployment** | **3.07** | |

Assessor’s Comment:

Technically sound practical systems and policies in place in line with quality standards and accepted best practices and legal requirements, fully implemented and regularly revised and updated. Main area of concern related to item GPB18 as mentioned in O9 above (Information Security Enhancement).

**Technical Best Practices – LAB #1:**

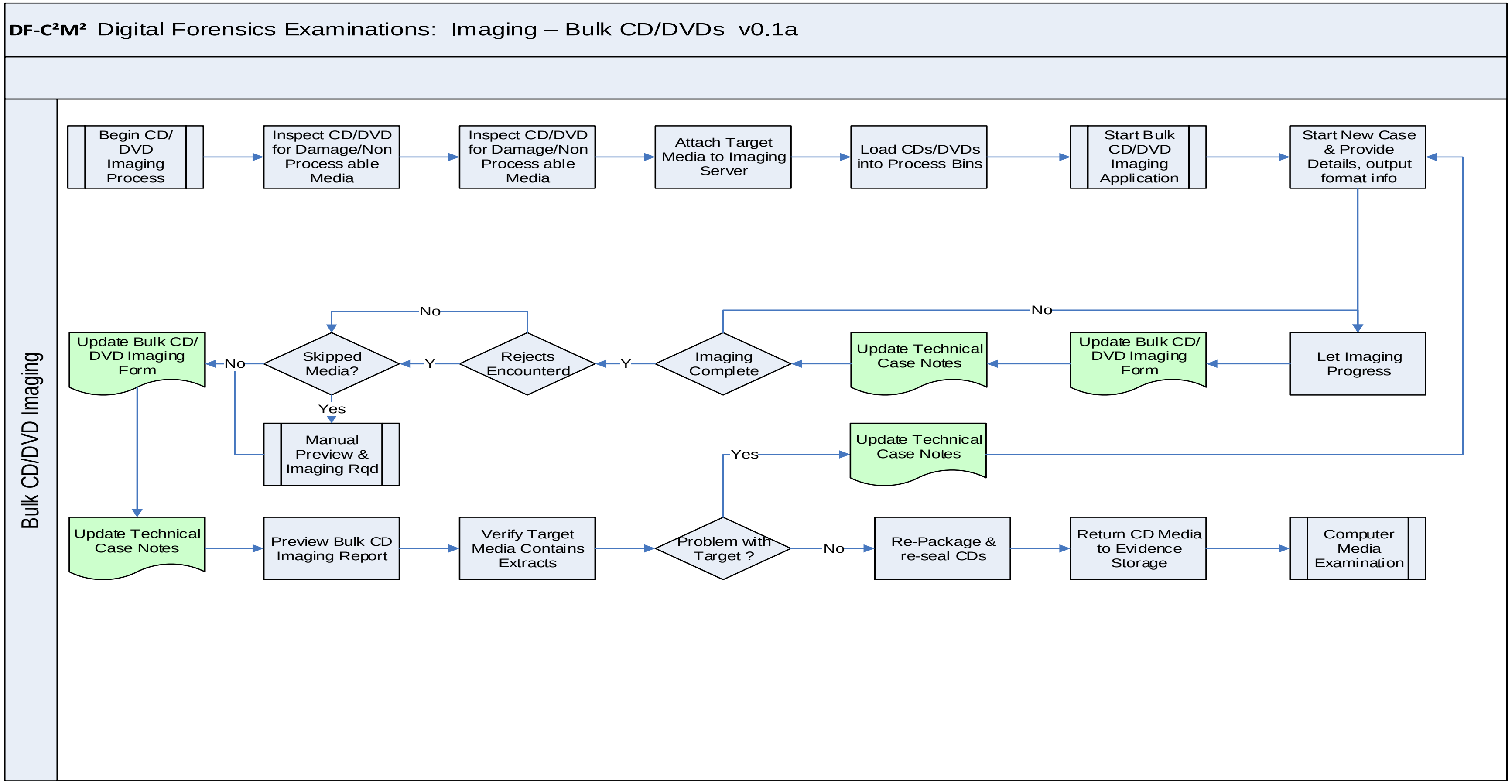
| Category | Description | Score | | |
|---|---|---|---|---|
| | | Level | Rating | Required |
| **TBP** | **Technical Best Practices** | | | |
| TBP1 | ACPO Principles | Level 5 - Continuously Improving | 5 | 5 |
| TBP2 | SWGDE Imaging | Level 4 - Measured & Automated | 4 | 5 |
| TBP3 | SWGDE Mobiles | Level 4 - Measured & Automated | 4 | 5 |
| TBP4 | Media Wiping | Level 4 - Measured & Automated | 4 | 5 |
| TBP5 | Encase | Level 4 - Measured & Automated | 4 | 5 |
| TBP6 | XWAYS | Level 4 - Measured & Automated | 4 | 5 |
| TBP7 | RAM Analysis | Level 4 - Measured & Automated | 4 | 5 |
| TBP8 | Workstation verification and performance testing (DFRWS) | Level 4 - Measured & Automated | 4 | 5 |
| TBP9 | Media Verification | Level 4 - Measured & Automated | 4 | 5 |
| | **Total Score** | | **37** | **45** |
| | **Maturity Level Average** | **Level 4 - Measured & Automated** | **4.11** | |

Assessor's Comment:

Technically sound practical systems and policies in place in line with quality standards and accepted best practices and legal requirements, fully implemented and regularly revised and updated.

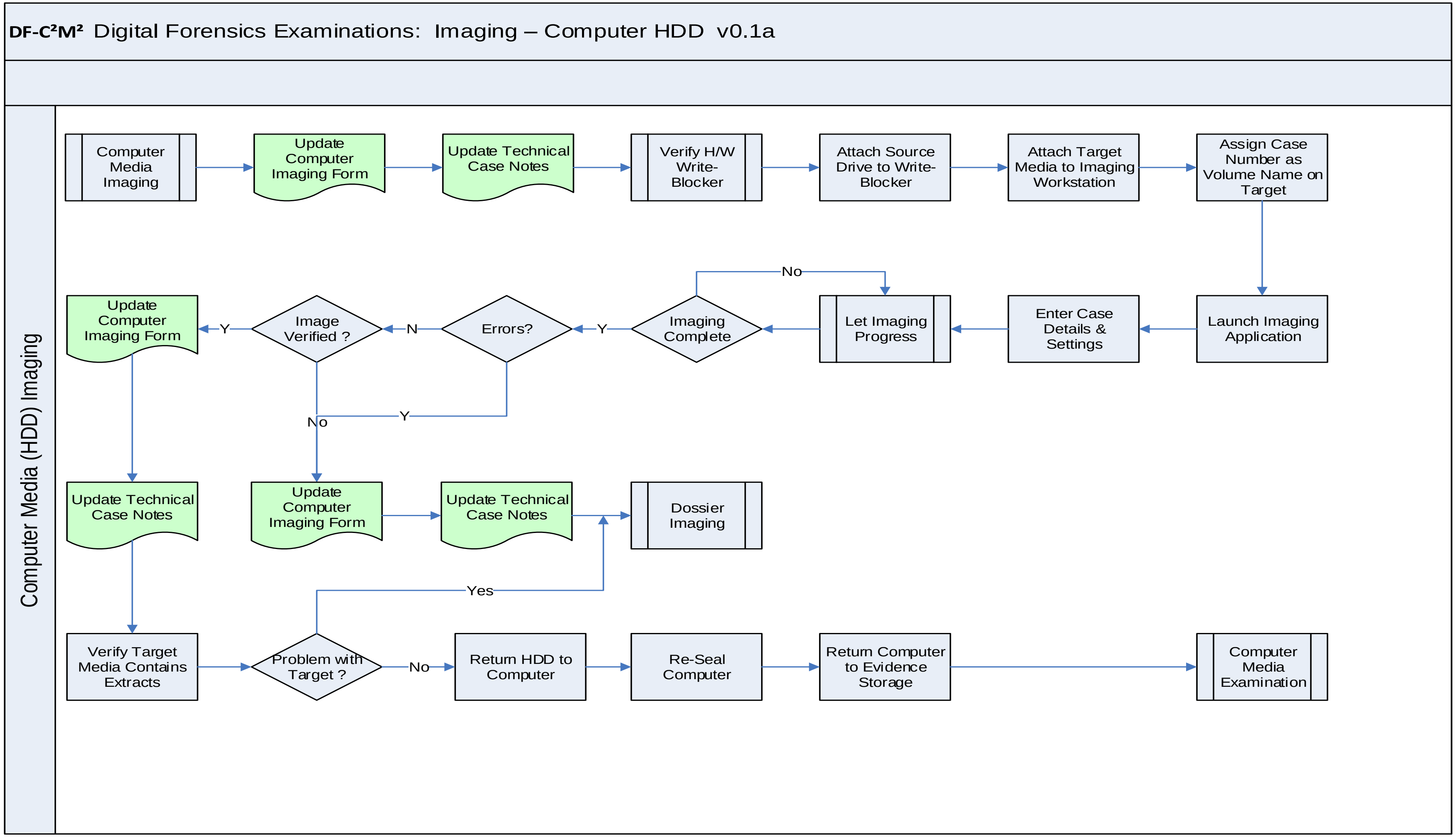
# APPENDIX F: DF-C²M² BODY OF KNOWLEDGE SAMPLE WORKFLOWS

## DF-C²M² Body of Knowledge Extracts: Bulk CD/DVD Media Imaging Process:

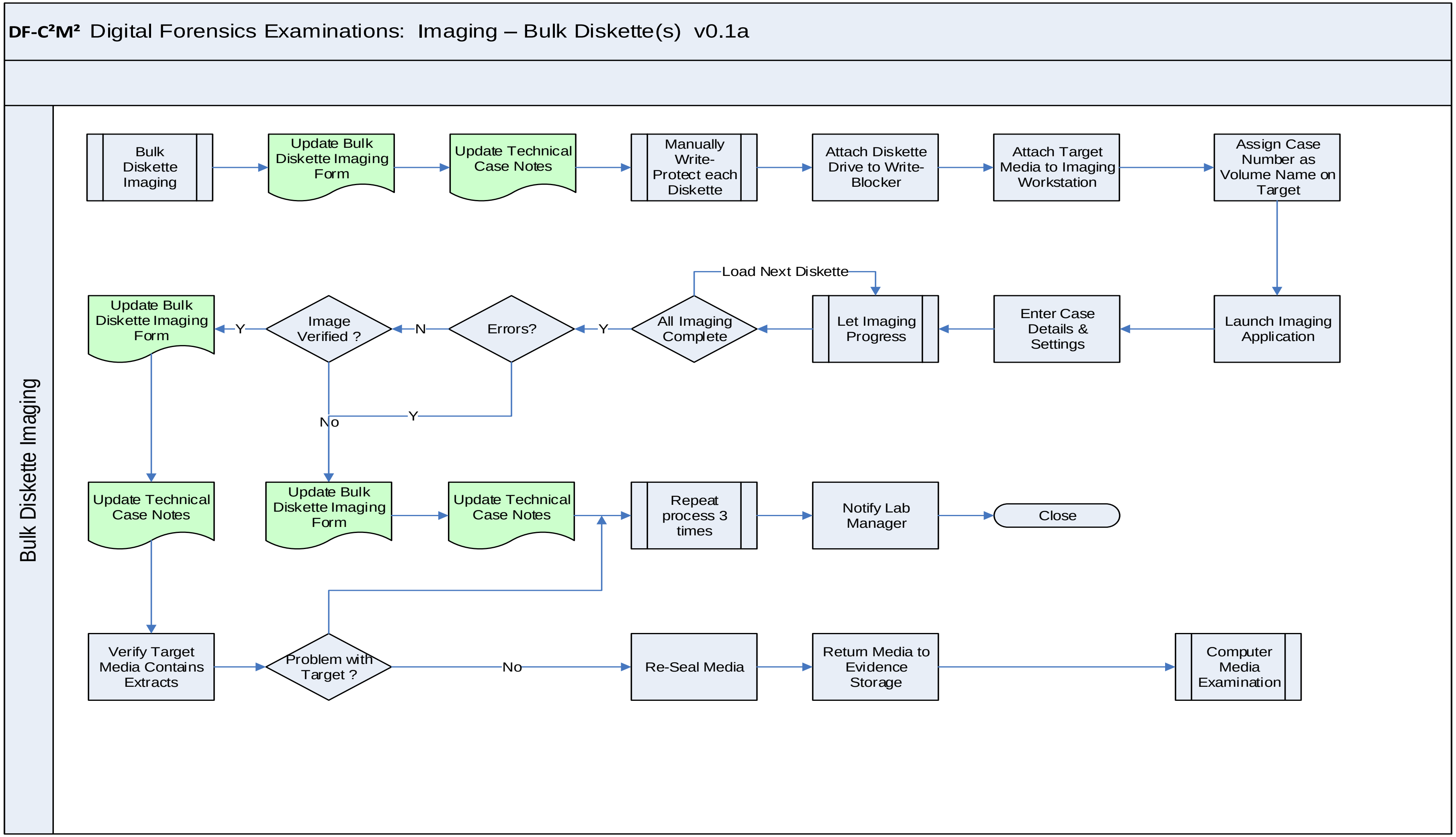


DF-C²M² Digital Forensics Examinations: Imaging – Bulk CD/DVDs v0.1a
Bulk CD/DVD Imaging
Begin CD/ DVD Imaging Process
Inspect CD/DVD for Damage/Non Process able Media
Inspect CD/DVD for Damage/Non Process able Media
Attach Target Media to Imaging Server
Load CDs/DVDs into Process Bins
Start Bulk CD/DVD Imaging Application
Start New Case & Provide Details, output format info
Let Imaging Progress
Update Bulk CD/ DVD Imaging Form
Update Technical Case Notes
Imaging Complete
No
Y
Rejects Encountered
No
Y
Skipped Media?
Yes
Manual Preview & Imaging Rqd
No
Update Bulk CD/ DVD Imaging Form
Update Technical Case Notes
Preview Bulk CD Imaging Report
Verify Target Media Contains Extracts
Problem with Target ?
Yes
Update Technical Case Notes
No
Re-Package & re-seal CDs
Return CD Media to Evidence Storage
Computer Media Examination

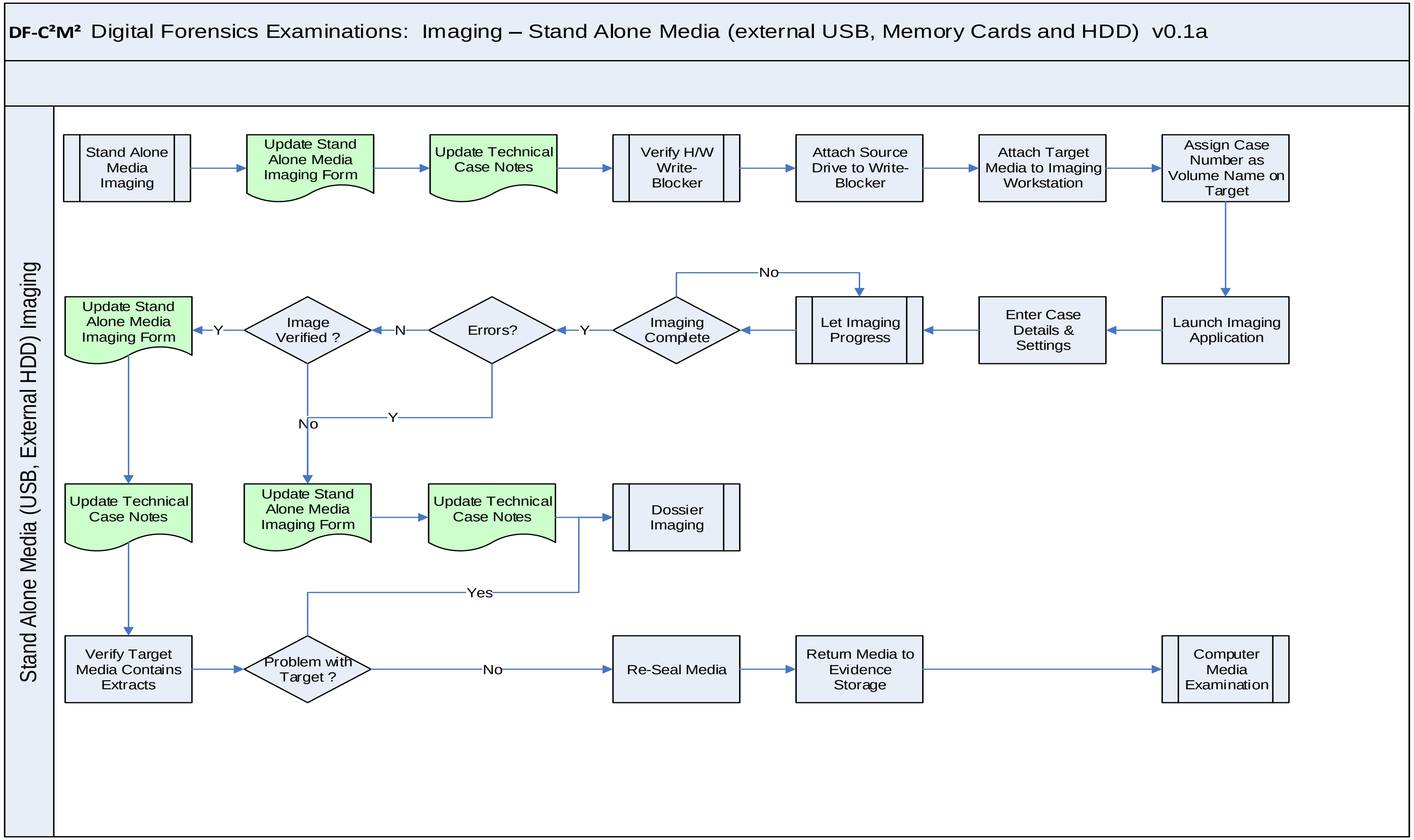
## DF-C²M² Body of Knowledge Extracts: Hard Disk Imaging process Overview:


DF-C²M² Digital Forensics Examinations: Imaging – Computer HDD v0.1a
Computer Media (HDD) Imaging
Computer Media Imaging
Update Computer Imaging Form
Update Technical Case Notes
Verify H/W Write-Blocker
Attach Source Drive to Write-Blocker
Attach Target Media to Imaging Workstation
Assign Case Number as Volume Name on Target
Launch Imaging Application
Enter Case Details & Settings
Let Imaging Progress
No
Imaging Complete
Y
Errors?
N
Image Verified ?
Y
Update Computer Imaging Form
Y
No
Update Technical Case Notes
Update Computer Imaging Form
Update Technical Case Notes
Dossier Imaging
Yes
Verify Target Media Contains Extracts
Problem with Target ?
No
Return HDD to Computer
Re-Seal Computer
Return Computer to Evidence Storage
Computer Media Examination

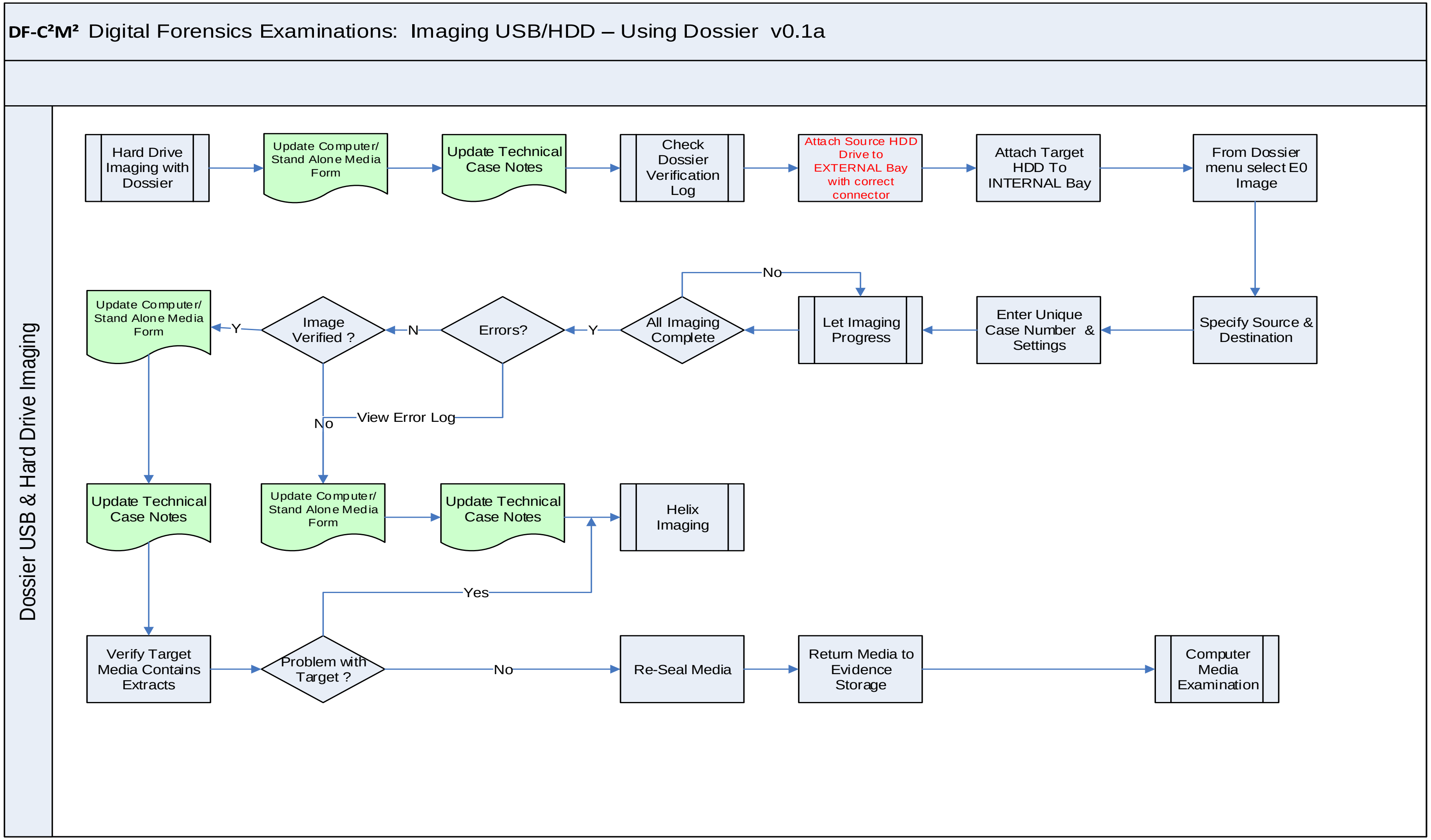
## DF-C²M² Body of Knowledge Extracts: Bulk Diskette Imaging Process Overview:


DF-C²M² Digital Forensics Examinations: Imaging – Bulk Diskette(s) v0.1a
Bulk Diskette Imaging
Bulk Diskette Imaging
Update Bulk Diskette Imaging Form
Update Technical Case Notes
Manually Write-Protect each Diskette
Attach Diskette Drive to Write-Blocker
Attach Target Media to Imaging Workstation
Assign Case Number as Volume Name on Target
Launch Imaging Application
Enter Case Details & Settings
Let Imaging Progress
Load Next Diskette
All Imaging Complete
Y
Errors?
N
Image Verified ?
Y
Update Bulk Diskette Imaging Form
Y
No
Update Technical Case Notes
Update Bulk Diskette Imaging Form
Update Technical Case Notes
Repeat process 3 times
Notify Lab Manager
Close
Verify Target Media Contains Extracts
Problem with Target ?
No
Re-Seal Media
Return Media to Evidence Storage
Computer Media Examination

## DF-C²M² Knowledge Base Extracts: Stand Alone Media Imaging Process Overview:

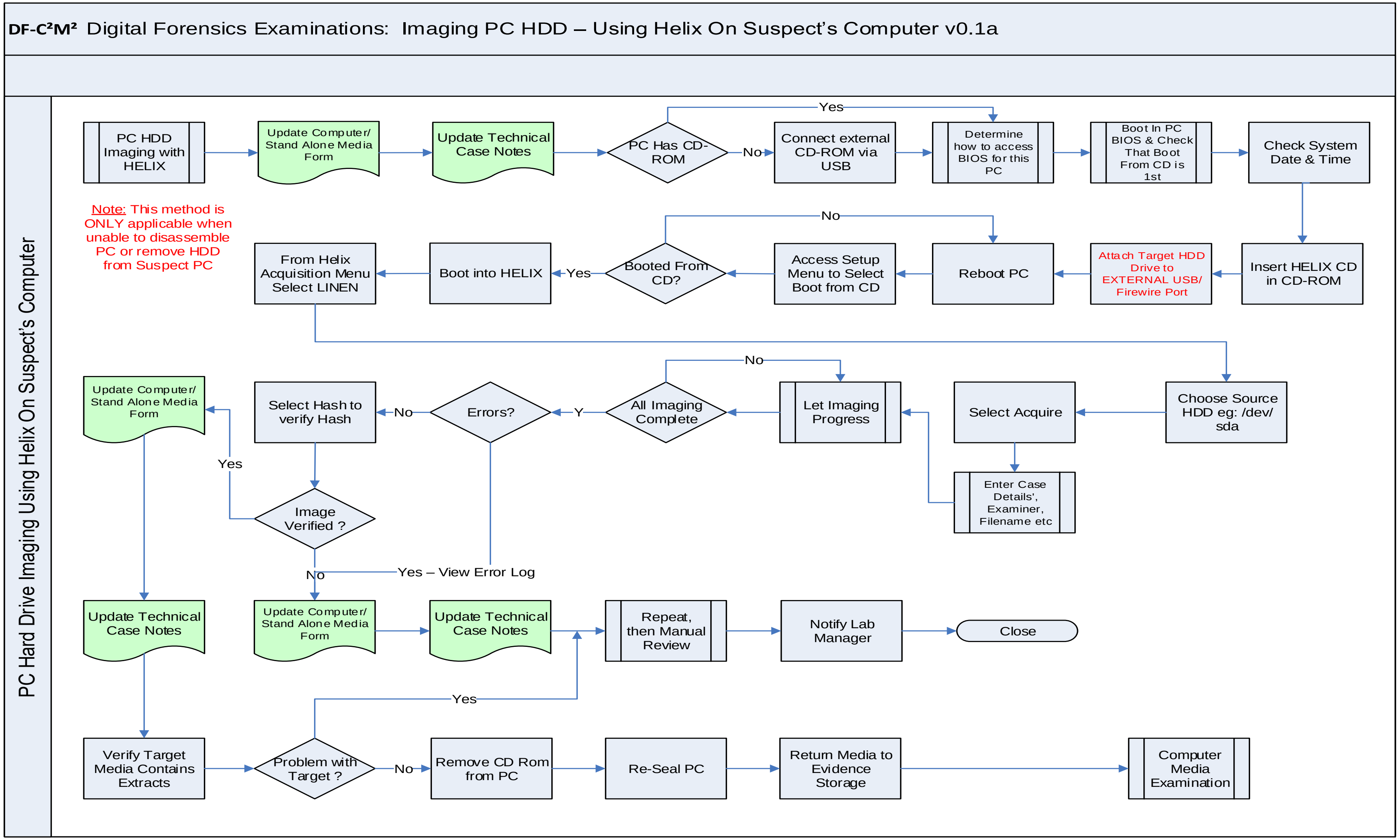

DF-C²M² Digital Forensics Examinations: Imaging – Stand Alone Media (external USB, Memory Cards and HDD) v0.1a
Stand Alone Media (USB, External HDD) Imaging
Stand Alone Media Imaging
Update Stand Alone Media Imaging Form
Update Technical Case Notes
Verify H/W Write-Blocker
Attach Source Drive to Write-Blocker
Attach Target Media to Imaging Workstation
Assign Case Number as Volume Name on Target
Launch Imaging Application
Enter Case Details & Settings
Let Imaging Progress
Imaging Complete
No
Y
Errors?
N
Y
Image Verified ?
Y
No
Update Stand Alone Media Imaging Form
Update Technical Case Notes
Update Stand Alone Media Imaging Form
Update Technical Case Notes
Dossier Imaging
Yes
Verify Target Media Contains Extracts
Problem with Target ?
No
Re-Seal Media
Return Media to Evidence Storage
Computer Media Examination

## DF-C²M² Knowledge Base Extracts: Media Imaging Using Dossier (Product-Specific) Overview:

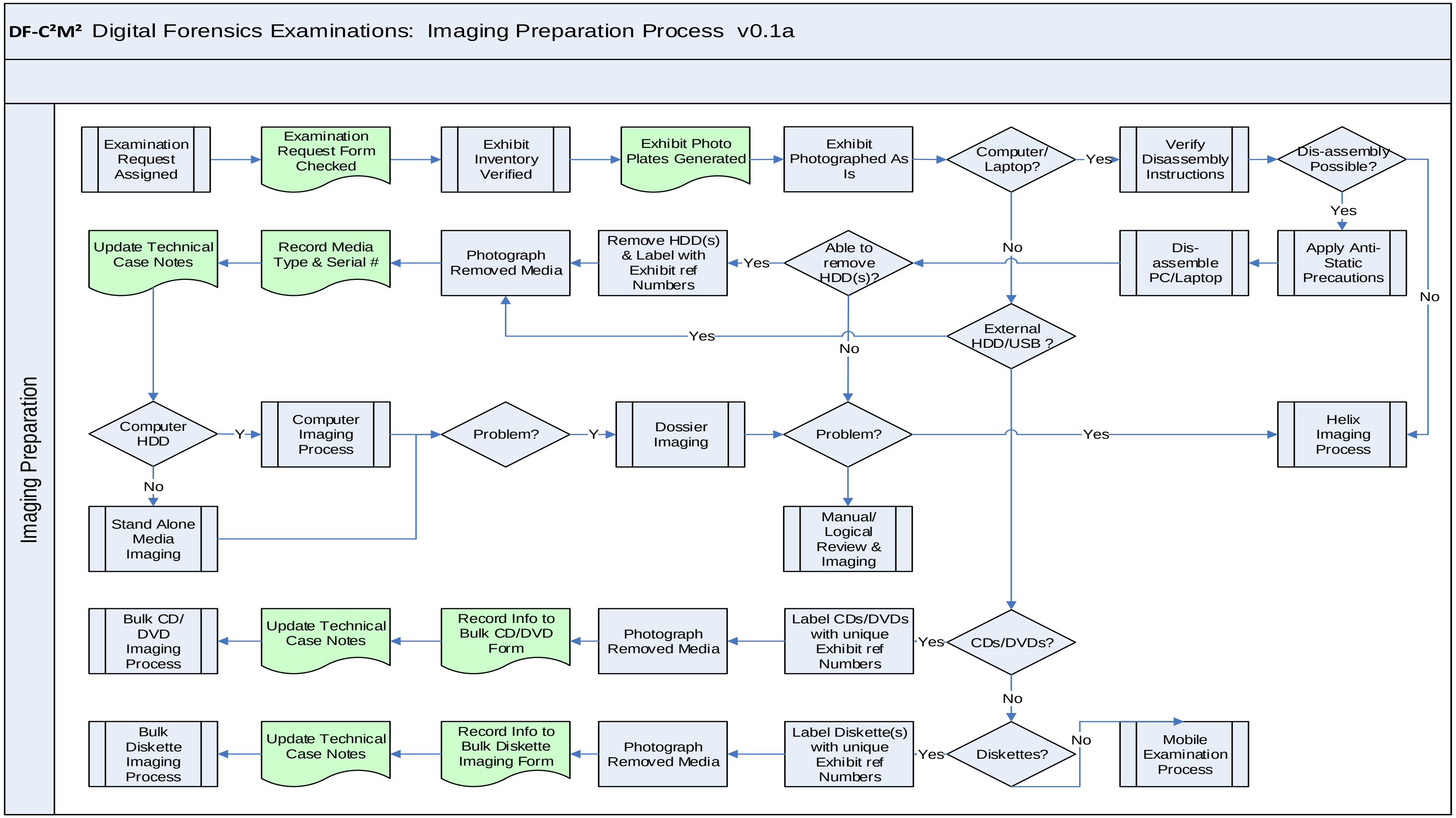


DF-C²M² Digital Forensics Examinations: Imaging USB/HDD – Using Dossier v0.1a
Dossier USB & Hard Drive Imaging
Hard Drive Imaging with Dossier
Update Computer/ Stand Alone Media Form
Update Technical Case Notes
Check Dossier Verification Log
Attach Source HDD Drive to EXTERNAL Bay with correct connector
Attach Target HDD To INTERNAL Bay
From Dossier menu select E0 Image
Specify Source & Destination
Enter Unique Case Number & Settings
Let Imaging Progress
No
All Imaging Complete
Y
Errors?
N
Image Verified ?
Y
Update Computer/ Stand Alone Media Form
View Error Log
No
Update Technical Case Notes
Update Computer/ Stand Alone Media Form
Update Technical Case Notes
Helix Imaging
Yes
Verify Target Media Contains Extracts
Problem with Target ?
No
Re-Seal Media
Return Media to Evidence Storage
Computer Media Examination

## DF-C²M² Knowledge Base Extracts: Using Helix (Method-1) Process Overview:


DF-C²M² Digital Forensics Examinations: Imaging PC HDD – Using Helix On Suspect's Computer v0.1a
PC Hard Drive Imaging Using Helix On Suspect's Computer
PC HDD Imaging with HELIX
Update Computer/ Stand Alone Media Form
Update Technical Case Notes
PC Has CD-ROM
No
Yes
Connect external CD-ROM via USB
Determine how to access BIOS for this PC
Boot In PC BIOS & Check That Boot From CD is 1st
Check System Date & Time
Note: This method is ONLY applicable when unable to disassemble PC or remove HDD from Suspect PC
Insert HELIX CD in CD-ROM
Attach Target HDD Drive to EXTERNAL USB/ Firewire Port
Reboot PC
Access Setup Menu to Select Boot from CD
Booted From CD?
No
Yes
Boot into HELIX
From Helix Acquisition Menu Select LINEN
Choose Source HDD eg: /dev/ sda
Select Acquire
Enter Case Details', Examiner, Filename etc
Let Imaging Progress
All Imaging Complete
No
Y
Errors?
No
Select Hash to verify Hash
Image Verified ?
Yes
Update Computer/ Stand Alone Media Form
No
Yes – View Error Log
Update Computer/ Stand Alone Media Form
Update Technical Case Notes
Repeat, then Manual Review
Notify Lab Manager
Close
Update Technical Case Notes
Verify Target Media Contains Extracts
Problem with Target ?
Yes
No
Remove CD Rom from PC
Re-Seal PC
Return Media to Evidence Storage
Computer Media Examination

## DF-C$^2$M$^2$ Knowledge Base Extracts: Imaging Preparation Process Overview:


DF-C²M² Digital Forensics Examinations: Imaging Preparation Process v0.1a
Imaging Preparation
Examination Request Assigned
Examination Request Form Checked
Exhibit Inventory Verified
Exhibit Photo Plates Generated
Exhibit Photographed As Is
Computer/ Laptop?
Yes
Verify Disassembly Instructions
Dis-assembly Possible?
Yes
No
Apply Anti-Static Precautions
Dis-assemble PC/Laptop
No
Able to remove HDD(s)?
Yes
Remove HDD(s) & Label with Exhibit ref Numbers
Photograph Removed Media
Record Media Type & Serial #
Update Technical Case Notes
External HDD/USB ?
Yes
No
Computer HDD
Y
No
Computer Imaging Process
Problem?
Y
Dossier Imaging
Problem?
Yes
Helix Imaging Process
Stand Alone Media Imaging
Manual/ Logical Review & Imaging
CDs/DVDs?
Yes
Label CDs/DVDs with unique Exhibit ref Numbers
Photograph Removed Media
Record Info to Bulk CD/DVD Form
Update Technical Case Notes
Bulk CD/ DVD Imaging Process
No
Diskettes?
Yes
No
Label Diskette(s) with unique Exhibit ref Numbers
Photograph Removed Media
Record Info to Bulk Diskette Imaging Form
Update Technical Case Notes
Bulk Diskette Imaging Process
Mobile Examination Process

# APPENDIX G: EVALUATION FORMS AND FEEDBACK

| | | Strongly Agree | Agree | Neither Agree Nor Disagree | Disagree | Strongly Disagree | |
|---|---|---|---|---|---|---|---|
| #1 | **Section:- General** | **5** | **4** | **3** | **2** | **1** | |
| 1. | There is a need for a set of an Internationally standardized best practices that cover the main areas related to Digital Forensics (People, Process, and Tools,) | ☒ | □ | □ | □ | □ | |
| | **Results:** All practitioners interviewed agreed unanimously to this point | | | | | | |
| 2. | Existing Models related to Digital Forensics are either too general or too specific and does not address key areas of importance. | ☒ | □ | □ | □ | □ | |
| | **Results:** 78% of respondents Strongly agreed to this point, with 22% Neither Agreeing nor disagreeing | | | | | | |
| 3. | The costs of developing all-encompassing Digital Forensics Policies and Procedures (in-line with International Best Practices) are seen by many to be too cost-prohibitive and time-consuming | ☒ | □ | □ | □ | □ | |
| | **Results:** All practitioners interviewed agreed unanimously to this point | | | | | | |
| 4. | The costs of implementing and maintaining all-encompassing Digital Forensics Policies and procedures in-line with International Best Practices are seen by many to be too time consuming and therefore cost prohibitive | □ | □ | ☒ | □ | □ | |
| | **Results:** 22% of respondents strongly agreed to this point, with 36% agreeing and 42% Neither Agreeing nor disagreeing to this point | | | | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 5. | Proposed standards from ISO under the 27000 series related to Digital Evidence and Forensic Analysis will contribute towards a more internationally accepted Digital Forensics Model, but do not address all the three key areas identified (People, Process, Tools) | ☐ | ☒ | ☐ | ☐ | ☐ | |
| | **Results:** 78% of respondents agreed to this point, with 22% Neither Agreeing nor disagreeing | | | | | | |
| 6. | Existing Standards applied to some digital Forensic Laboratories such as ASCLD-LAB, or ISO/IEC:17025 are ill-suited to the specialist field of Digital Forensics | ☐ | ☐ | ☒ | ☐ | ☐ | |
| | **Results:** 78% of respondents agreed to this point with 22% neither Agreeing nor disagreeing | | | | | | |
| 7. | Existing Digital Forensic Models do not fully address the following key areas: People (including skills development, and proficiency testing), Processes (Based on accepted Best Practices or legal requirements), and the use of validation of Tools and Methods | ☐ | ☒ | ☐ | ☐ | ☐ | |
| | **Results:** 64% of respondents agreed to this point, with 14% neither Agreeing nor disagreeing and 22% disagreeing | | | | | | |
| 8. | An internationally standardized model for Digital Forensics is Laboratories and Practitioners is needed and will help stream-line and standardize the field of Digital Forensics to level on par with that of other forensic disciplines | ☐ | ☒ | ☐ | ☐ | ☐ | |
| | **Results:** All respondents unanimously agreed to this point. | | | | | | |
| 9. | An internationally standardized model for Digital Forensics may be too restrictive, and therefore a flexible model/ framework that can | ☐ | ☒ | ☐ | ☐ | ☐ | |
| | **Results:**85% of respondents agreed to this point with 15% disagreeing | | | | | | |

|  |  | Strongly Agree | Agree | Neither Agree Nor Disagree | Disagree | Strongly Disagree |  |
|---|---|---|---|---|---|---|---|
| #2 | Section 2:- DF-C$^2$M$^2$ - Organisation | 5 | 4 | 3 | 2 | 1 |  |
| 1. | The proposed model covers Organizational requirements in sufficient depth/detail | ☐ | ☒ | ☐ | ☐ | ☐ |  |
|  | **Results:** All respondents unanimously agreed to this point. |  |  |  |  |  |  |
| 2. | The proposed model cater for all aspects of Law Enforcement and Non-Law Enforcement Organizational Requirements | ☐ | ☒ | ☐ | ☐ | ☐ |  |
|  | **Results:** All respondents unanimously agreed to this point. |  |  |  |  |  |  |
| 3. | Forensic Readiness is a key area often neglected in many Organisational plans/strategies | ☒ | ☐ | ☐ | ☐ | ☐ |  |
|  | **Results:** All respondents strongly agreed to this point. |  |  |  |  |  |  |
| 4. | The Organisational requirements for both Law Enforcement(LE) and NON-LE Organisations are practical | ☐ | ☒ | ☐ | ☐ | ☐ |  |
|  | **Results:** 85% of respondents agreed to this point with 15% neither Agreeing nor disagreeing |  |  |  |  |  |  |
| 5. | The Organisational requirements for both Law Enforcement and NON-LE Organisations are achievable for most organisations | ☐ | ☒ | ☐ | ☐ | ☐ |  |
|  | **Results:** 78% of respondents agreed to this point with 22% neither Agreeing nor disagreeing |  |  |  |  |  |  |
| 6. | The Organisational requirements within the model overlooks certain critical elements that should be included | ☐ | ☐ | ☐ | ☐ | ☐ |  |
|  | **Results:** 71% of respondents disagreed to this point with 15% neither agreeing nor disagreeing, and 14% agreeing |  |  |  |  |  |  |
| 7. | The Overall Requirements of the model will assist in clearly defining the requirements for an effective and efficient Digital Forensic Lab/Capability within an organisation | ☐ | ☒ | ☐ | ☐ | ☐ |  |
|  | **Results:** 78% of respondents agreed to this point with 22% neither Agreeing nor disagreeing. |  |  |  |  |  |  |

|  |  | **Strongly Agree** | **Agree** | **Neither Agree Nor Disagree** | **Disagree** | **Strongly Disagree** |  |
|---|---|---|---|---|---|---|---|
| #3 | Section 3:- DF-C$^2$M$^2$ - Service Catalogue | 5 | 4 | 3 | 2 | 1 |  |
| 1. | The concept of establishing a Service Catalogue helps to identify the possible range of typical requirements and plan for the introduction and readiness of each listed service | ☒ | □ | □ | □ | □ |  |
|  | **Results:** All respondents strongly agreed to this point. |  |  |  |  |  |  |
| 2. | The sample proposed Service Catalogue allows organisations to help define the People, Policy, Tools requirements for each service | □ | ☒ | □ | □ | □ |  |
|  | **Results:** All respondents agreed to this point. |  |  |  |  |  |  |
| 3. | The Service Catalogue Impact vs. Complexity analysis allows organisations to plan to identify limitations and advantages of each proposed service in sufficient detail. | □ | ☒ | □ | □ | □ |  |
|  | **Results:** 85% of respondents agreed to this point with 15%  strongly agreeing |  |  |  |  |  |  |
| 4. | Non-standard/typical Digital Forensic services should be removed from the Service Catalogue | □ | □ | ☒ | □ | □ |  |
|  | **Results:** 78% of respondents neither Agreed nor disagreed to this point, with 22% agreeing |  |  |  |  |  |  |
| 5. | An industry-wide common catalogue of services that defines (People, Process, Tools,) requirements of each service, as well as impact vs. complexity rating would be very useful. | □ | ☒ | □ | □ | □ |  |
|  | **Results:** All respondents unanimously agreed to this point |  |  |  |  |  |  |
| 6. | Clearly identifying the requirements and limitations of each services as well as Service Level Targets will help improved overall customer awareness, and satisfaction | □ | ☒ | □ | □ | □ |  |
|  | **Results:** All respondents unanimously agreed to this point |  |  |  |  |  |  |
| 7. | Categorizing the services in the Service Catalogue based on areas of expertise e.g.: Computer Forensics, Mobile Forensics, etc. will allow organisations to easily identify which service areas apply to them organizational needs and which areas to focus on | ☒ | □ | □ | □ | □ |  |
|  | **Results:** All respondents unanimously strongly agreed to this point |  |  |  |  |  |  |

| | | Strongly Agree | Agree | Neither Agree Nor Disagree | Disagree | Strongly Disagree | |
|---|---|---|---|---|---|---|---|
| #4 | Section 4:- DF-C$^2$M$^2$ - People | 5 | 4 | 3 | 2 | 1 | |
| 1. | The proposed model clearly identifies the various roles within a typical Digital Forensic Lab/Facility | ☐ | ☒ | ☐ | ☐ | ☐ | |
| | **Results:** 85% of respondents agree to this point with 15% neither agreeing nor disagreeing | | | | | | |
| 2. | The People Capability Maturity Model is sufficiently well defined and is suited to the specialist field of digital forensics. | ☐ | ☐ | ☐ | ☐ | ☐ | |
| | **Results:** 64% of respondents agree to this point, with 28% neither agreeing nor disagreeing and 7% strongly agreeing with this point | | | | | | |
| 3. | The proposed model provide a structured and easy to implement way to assess, measure and benchmark skills for DF personnel | ☐ | ☒ | ☐ | ☐ | ☐ | |
| | **Results:** All respondents agreed unanimously to this point | | | | | | |
| 4. | On the People Capability Maturity - A minimum DF-C$^2$M$^2$ target of 3 is sufficient to meet the requirements of most digital forensic labs. | ☐ | ☒ | ☐ | ☐ | ☐ | |
| | **Results:** 71% of respondents agree to this point, with 14% agreeing strongly and 25% neither agreeing nor disagreeing | | | | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 5. | The proposed model’s concept of benchmarking skill sets results against other participating labs, whilst ensuring individual and organizational confidentiality will allow for more accurate testing and benchmarking of labs and their efficiency/competency of their personnel | ☒ | □ | □ | □ | □ | |
| | **Results:** All respondents agreed unanimously to this point | | | | | | |
| 6. | The concept of including People Capability Maturity within the model allows for organisations to plan for, and achieve greater overall efficiency in the intermediate future (2-3 years) | □ | □ | □ | □ | □ | |
| | **Results:** 64% of respondents agree to this point, with 35% neither agreeing nor disagreeing | | | | | | |
| 7. | The proposed maturity model and ratings are both practical and achievable for most organisations. The definitions and details regarding the People Capability Maturity are sufficiently detailed in explanation | □ | □ | □ | □ | □ | |
| | **Results:** 71% of respondents agree to this point, with 14% neither agreeing nor disagreeing, and 15% disagreeing | | | | | | |

|  |  | Strongly Agree | Agree | Neither Agree Nor Disagree | Disagree | Strongly Disagree |  |
|---|---|---|---|---|---|---|---|
| #5 | Section 5:- DF-C$^2$M$^2$ - Processes | 5 | 4 | 3 | 2 | 1 |  |
| 1. | Streamlined Processes (Policies and procedures) are key to establishing efficiency and integrity within a Digital Forensic Lab/facility | ☒ | ☐ | ☐ | ☐ | ☐ |  |
|  | **Results:** All respondents agreed strongly unanimously to this point |  |  |  |  |  |  |
| 2. | The requirement to ensure that all relevant policies and procedures are best of accepted best practices is vital to helping ensure integrity of the results produced by the facility | ☒ | ☐ | ☐ | ☐ | ☐ |  |
|  | **Results:** All respondents agreed unanimously to this point |  |  |  |  |  |  |
| 3. | Policies and procedures should be customizable by the DF facility as long as these changes to not affect the integrity (forensics soundness) of the policy, procedure method | ☒ | ☐ | ☐ | ☐ | ☐ |  |
|  | **Results:** All respondents agreed unanimously to this point |  |  |  |  |  |  |
| 4. | A standardized library of vetted, regularly updated set of policies and procedures based on best practices and any relevant standards (as part of the DF-C$^2$M$^2$ Body of Knowledge) will be a welcome aspect of the model for many participants | ☒ | ☐ | ☐ | ☐ | ☐ |  |
|  | **Results:** All respondents agreed unanimously to this point |  |  |  |  |  |  |
| 5. | Relevant ISO standards should be included within the DF-C$^2$M$^2$ Body of Knowledge/Policies and procedures if the Review committee/participating DF facilities feel they will add value. | ☐ | ☒ | ☐ | ☐ | ☐ |  |
|  | **Results:** 64% of respondents agree to this point, with 35% neither agreeing nor disagreeing |  |  |  |  |  |  |
| 6. | The DF-C$^2$M$^2$ Body of Knowledge should be submitted to a standards/regulatory body for validation and for the creation of a proposed accreditation and certification model for participating labs. | ☐ | ☒ | ☐ | ☐ | ☐ |  |
|  | **Results:** 72% of respondents agree to this point, with 28% neither agreeing nor disagreeing |  |  |  |  |  |  |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 7. | The DF-C$^2$M$^2$ Body of Knowledge should allow for authorised translations of the Processes into non-English languages | ☐ | ☒ | ☐ | ☐ | ☐ | |
| | **Results:** All respondents agreed unanimously to this point | | | | | | |
| 8. | Distribution of any Processes related to Law Enforcement-specific methods/tools should be restricted and not included in the DF-C$^2$M$^2$ Body of Knowledge for non-law Enforcement organisations | ☐ | ☒ | ☐ | ☐ | ☐ | |
| | **Results:** 71% of respondents agree to this point, with 14% agreeing strongly and 25% neither agreeing nor disagreeing | | | | | | |
| 9. | The proposed processes and policies within the DF-C$^2$M$^2$ Body of Knowledge should provide a framework to allow any local regulatory requirements or international standards requirements to be added to the framework with minimal disruption and at minimal cost to practicality DF facilities | ☐ | ☒ | ☐ | ☐ | ☐ | |
| | **Results:** 72% of respondents agree to this point, with 28% neither agreeing nor disagreeing | | | | | | |
| 10. | The DF-C$^2$M$^2$ Six Steps Model is both practical and it covers all aspects of Digital Forensics Examination Life Cycle. | ☐ | ☒ | ☐ | ☐ | ☐ | |
| | **Results:** All respondents unanimously agree to this point. | | | | | | |
| 11. | Acceptance of the proposed DF-C$^2$M$^2$ processes within the DF-C$^2$M$^2$ Body of Knowledge should be by peer-review of participating DF facilities and any other suitably qualified 3rd parties. Processes defined with the DF-C$^2$M$^2$ Body of Knowledge should be reviewed at least annually and updates published to participating DF facilities | ☒ | ☐ | ☐ | ☐ | ☐ | |
| | **Results:** All respondents strongly agree to this point. | | | | | | |
| 12. | Overall the DF-C$^2$M process criteria is sufficiently detailed and in-line with existing best practices | ☐ | ☒ | ☐ | ☐ | ☐ | |

|  |  | Strongly Agree | Agree | Neither Agree Nor Disagree | Disagree | Strongly Disagree |  |
|---|---|---|---|---|---|---|---|
| **#6** | **Section 6:- DF-C$^2$M$^2$ - Tools** | **5** | **4** | **3** | **2** | **1** |  |
| 1. | Validation of tools and methods as defined within the Model are vital and essential to the integrity of a DF facility | ☒ | □ | □ | □ | □ |  |
|  | **Results:** All respondents strongly agree to this point. |  |  |  |  |  |  |
| 2. | Validations of tools and methods by testing and adoption of test results by DF-C$^2$M$^2$ participating labs will allow for better and faster testing of new tools and methods, and allow DF facilities to adopt newer tools and methods quicker, at reduced cost (of testing) | □ | ☒ | □ | □ | □ |  |
|  | **Results:** All respondents agreed to this point. |  |  |  |  |  |  |
| 3. | Publishing of the DF-C$^2$M$^2$ validation testing of tools and methods should be restricted to participating members and affected 3rd party vendors (where appropriate) | □ | ☒ | □ | □ | □ |  |
|  | **Results:** 64% respondents agreed to this point with 36% neither agreeing nor disagreeing |  |  |  |  |  |  |
| 4. | Inclusion of NIST tested tools should be a key element of the tool testing criteria (where applicable) | □ | ☒ | □ | □ | □ |  |
|  | **Results:** 71% of respondents agree to this point, with 29% neither agreeing nor disagreeing |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|---|
| 5. | Participating DF facilities should have the right to have custom tools tested by only selected 3rd parties (and results shared only amongst those participants under suitable NDAs) | □ | □ | ☒ | □ | □ |  |
|  | **Results:** 50% of respondents agree to this point, with 50% neither agreeing nor disagreeing |  |  |  |  |  |  |
| 6. | The DF-C²M² proposed tool testing requirements are in line with accepted international best practices | □ | ☒ | □ | □ | □ |  |
|  | **Results:** 72% of respondents agree to this point, with 28% neither agreeing nor disagreeing |  |  |  |  |  |  |
| 7. | Overall the DF-C²M² adequately addresses the tool and methods validation requirements in line with exiting best practices | □ | □ | □ | □ | □ |  |
|  | **Results:** All respondents agreed to this point. |  |  |  |  |  |  |

|  |  | **Strongly Agree** | **Agree** | **Neither Agree Nor Disagree** | **Disagree** | **Strongly Disagree** |  |
|---|---|---|---|---|---|---|---|
| #7 | Section 7:- DF-C$^2$M$^2$ - Overall feedback | 5 | 4 | 3 | 2 | 1 |  |
| 1 | The DF-C$^2$M$^2$ provides a sound framework and set of requirements for the People aspect of an Internationally reputed DF facility | □ | ☒ | □ | □ | □ |  |
|  | **Results:** All respondents agreed to this point. |  |  |  |  |  |  |
| 2 | The DF-C$^2$M$^2$ provides a sound framework and set of requirements for the Processes aspect of an Internationally reputed DF facility | ☒ | □ | □ | □ | □ |  |
|  | **Results:** All respondents strongly agreed to this point. |  |  |  |  |  |  |
| 3 | The DF-C$^2$M$^2$ provides a sound framework and set of requirements for the testing of Tools and Methods aspect of an Internationally reputed DF facility | □ | ☒ | □ | □ | □ |  |
|  | **Results:** All respondents agreed to this point. |  |  |  |  |  |  |
| 4 | The DF-C$^2$M$^2$ provides a sound framework and set of requirements for the Organizational aspect of an Internationally reputed DF facility | □ | ☒ | □ | □ | □ |  |
|  | **Results:** All respondents agreed to this point. |  |  |  |  |  |  |
| 5 | The DF-C$^2$M$^2$ is a implementable (with the DF-C$^2$M$^2$ Body of Knowledge) for the majority of organisations | □ | ☒ | □ | □ | □ |  |
|  | **Results:** 72% of respondents agree to this point, with 28% neither agreeing nor disagreeing |  |  |  |  |  |  |
| 6 | The DF-C$^2$M$^2$ will provide value and cost savings to many organisations | □ | ☒ | □ | □ | □ |  |
|  | **Results:** All respondents agreed to this point. |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|---|
| 7 | The DF-C$^2$M$^2$ is viable as a proposed international standard/framework | ☐ | ☒ | ☐ | ☐ | ☐ |  |
|  | **Results:** 71% of respondents agree to this point, with 29% neither agreeing nor disagreeing |  |  |  |  |  |  |
| 8 | The proposed DF-C$^2$M$^2$ will allow organisations that have or plan to implement Digital Forensic capabilities to become more proficient? | ☐ | ☒ | ☐ | ☐ | ☐ |  |
|  | **Results:** 78% of respondents agree to this point, with 22% neither agreeing nor disagreeing |  |  |  |  |  |  |
| 9 | The proposed DF-C$^2$M$^2$ will allow organisations that have or plan to implement Digital Forensic capabilities to improve the overall levels of competency within their digital forensic laboratories | ☐ | ☒ | ☐ | ☐ | ☐ |  |
|  | **Results:** 78% of respondents agree to this point, with 22% neither agreeing nor disagreeing |  |  |  |  |  |  |
| 10 | The DF-C$^2$M$^2$ be structured as a Framework rather than a Model | ☒ | ☐ | ☐ | ☐ | ☐ |  |
|  | **Results:** 71% of respondents strongly agreed to this point, with 29% neither agreeing nor disagreeing |  |  |  |  |  |  |
| 11 | The DF-C$^2$M$^2$ will prove to be useful to existing Digital Forensic Labs | ☒ | ☐ | ☐ | ☐ | ☐ |  |
|  | **Results:** All respondents agreed to this point. |  |  |  |  |  |  |

# APPENDIX H: CFTT /NIST SPECIFICATION DEVELOPMENT PROCESS

After a tool category and at least one tool is selected by the steering committee, the development process is as follows:

1. NIST and law enforcement staff develops a requirements, assertions and test cases document (called the tool category specification).
2. The tool category specification is posted to the web for peer review by members of the computer forensics community and for public comment by other interested parties.
3. Relevant comments and feedback are incorporated into the specification.
4. A test environment is designed for the tool category.

CFTT Tool test process

After a category specification has been developed and a tool selected, the test process is as follows:

1. NIST acquires the tool to be tested.
2. NIST reviews the tool documentation.
3. NIST selects relevant test cases depending on features supported by the tool.
4. NIST develops test strategy.
5. NIST executes tests
6. NIST produces test report.
7. Steering Committee reviews test report.
8. Vendor reviews test report.
9. NIST posts support software to web.
10. DHS posts test report to web.

# APPENDIX I: ETHICS APPROVAL

**From:** Ethics (RSO) Enquiries

**Sent:** Wednesday, May 23, 2012 6:14 PM

**To:** Al Hanaei, Ebrahim Hamad Salem <alhanaei@exchange.lancs.ac.uk>

**Cc:** 'Awais Rashid' <marash@comp.lancs.ac.uk>

**Subject:** Stage 1 self-assessment approval

Dear Ebrahim

Thank you for submitting your completed stage 1 self-assessment form for **Qualifying digital forensics specialists: towards a comprehensive model for the digital forensics profession** and the additional information which we requested. The Part B information has been reviewed by the Chair of the University Research Ethics Committee and I can confirm that approval has been granted for this project.

As principal investigator your responsibilities include:

- ensuring that (where applicable) all the necessary legal and regulatory requirements in order to conduct the research are met, and the necessary licenses and approvals have been obtained;
- reporting any ethics-related issues that occur during the course of the research or arising from the research (e.g. unforeseen ethical issues, complaints about the conduct of the research, adverse reactions such as extreme distress) to the Research Ethics Officer;
- Submitting details of proposed substantive amendments to the protocol to the Research Ethics Officer for approval.

Please contact the Research Ethics Officer, Debbie Knight (ethics@lancaster.ac.uk 01542 592605) if you have any queries or require further information.

Kind regards,

*Debbie*

Debbie Knight

Research Ethics Officer

Research Support Office

B58, B Floor,

Bowland Main

Lancaster University

Lancaster, LA1 4YT

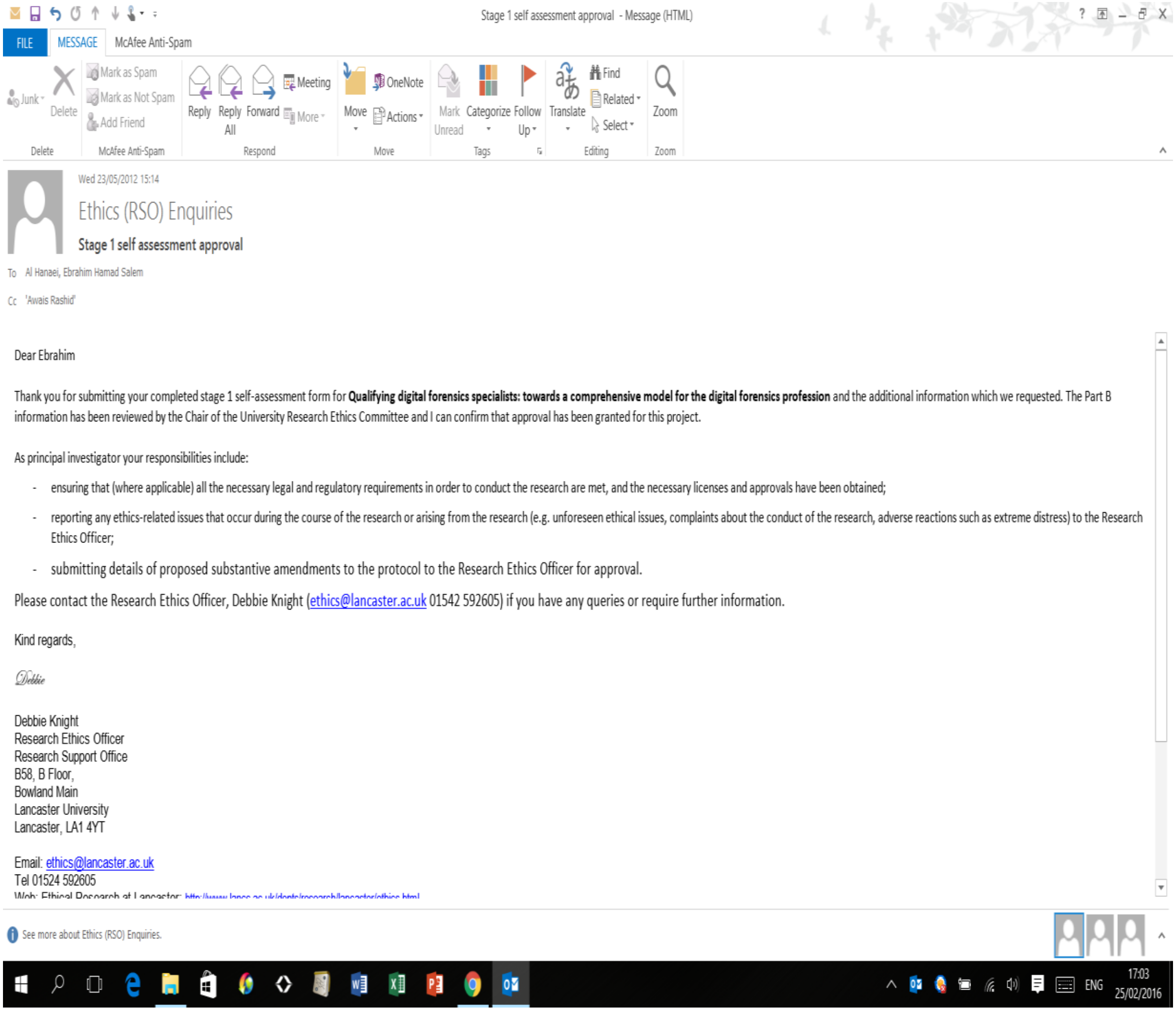
Email: ethics@lancaster.ac.uk

Tel 01524 592605

Web: Ethical Research at Lancaster: http://www.lancs.ac.uk/depts/research/lancaster/ethics.html

**Looking for funding opportunities specific to your research?**

**Go to the RSO website to search the *Research Professional* funding database.**



Wed 23/05/2012 15:14

Ethics (RSO) Enquiries

Stage 1 self assessment approval

To Al Hanaei, Ebrahim Hamad Salem

Cc 'Awais Rashid'

Dear Ebrahim

Thank you for submitting your completed stage 1 self-assessment form for **Qualifying digital forensics specialists: towards a comprehensive model for the digital forensics profession** and the additional information which we requested. The Part B information has been reviewed by the Chair of the University Research Ethics Committee and I can confirm that approval has been granted for this project.

As principal investigator your responsibilities include:

- ensuring that (where applicable) all the necessary legal and regulatory requirements in order to conduct the research are met, and the necessary licenses and approvals have been obtained;
- reporting any ethics-related issues that occur during the course of the research or arising from the research (e.g. unforeseen ethical issues, complaints about the conduct of the research, adverse reactions such as extreme distress) to the Research Ethics Officer;
- submitting details of proposed substantive amendments to the protocol to the Research Ethics Officer for approval.

Please contact the Research Ethics Officer, Debbie Knight (ethics@lancaster.ac.uk 01542 592605) if you have any queries or require further information.

Kind regards,

Debbie

Debbie Knight
Research Ethics Officer
Research Support Office
B58, B Floor,
Bowland Main
Lancaster University
Lancaster, LA1 4YT

Email: ethics@lancaster.ac.uk
Tel 01524 592605
Web: Ethical Research at Lancaster: http://www.lancs.ac.uk/depts/research/lancaster/ethics.html

# APPENDIX J: INDUSTRY BEST PRACTICES

The following industry best practices were referenced and use as guides for the Body of Knowledge and Assessment Tool evaluation criteria:

**Scientific Working Group on Digital Evidence (SWGDE):**

- 2006-01-20 SWGDE Proficiency Test Guidelines
- SWGDE SOP for Computer Forensics v2
- 2007-02-06 SWGDE Capture of Live Systems v.1
- 2011-06-17 SWGDE Model QAM for Digital Evidence Laboratories v1
- 2009-01-15 SWGDE Recommendations for Validation Testing Version
- 2013-02-11 SWGDE Best Practices for Mobile Phone Forensics V2-0
- 2013-02-11 SWGDE Core Competencies for Mobile Phone Forensics V1-0
- 2012-09-12 SWGDE Best Practices for Portable GPS Devices V1-1
- 2011-09-15 SWGDE Core Competencies for Forensic Audio v1
- 2010-01-15 SWGDE-SWGIT Guidelines and Recommendations for Training v2.0
- 2010-05-15 SWGDE Min Req. for QA in Proc Digital Multimedia Evidence_v1

**Note: Several of the above Best practices have been updated since this research was initially performed.**

**APCO:** Good Practice Guide for Digital Evidence

**NIST:**

- NIST SP-800-86 Guide to Integrating Forensic Techniques into Incident Response
- NIST SP-800-109 Guidelines on Mobile Device Forensics

**NIJ:**

- Forensic Examination of Digital Evidence: A Guide for Law Enforcement
- ASCLD-LAB: Supplement Requirements to ISO 17025
- Encase EnCE Study Guide – Steve Bunting
- AccessData FTK v3 Training Manual
- Xways Forensics Training Manual
- XRY Mobile Forensics Training Manual

# REFERENCES

A2LA. (2013, 10 18). *American Association for Laboratory Accreditation.* Retrieved 2 29, 2014, from R103a – Annex – Proficiency Testing for ISO/IEC 17025 Laboratories document: https://www.a2la.org/requirements/Annex_to_the_A2LA_General_Requirements_for_Proficiency_Testing.pdf

ACE, A. C. (n.d.). Retrieved 2013, from http://accessdata.com/services/digital-forensics.

Adams, R. B. (2012). *The Dvanced Data Acquisition Model (ADAM): A process Model for Digital Forenisc Practice.* Richard Brian Adams.

Adams, Whitledge, & Shenoi. (2008). Legal Issues Pertaining to teh Use of Cell Phone Data. *Advances in Digital Forensics IV*, 231-246.

Agarwal, Gupta, Saurabh, G., & Gupta, P. (. (2011). Systematic Digital Forensic Investigation Model. *International Journal of Computer Science and Security (IJCSS), Volume (5) : Issue (1).*

Al_Hanaee, E. A., & Rashid, A. (2014). DF-C²M²: A Capability Maturity Model for Digital Forensics Organisations. *IEEE Security and Privacy Workshops 2014*, 57-60.

American Association for Laboratory Accreditation. (2013, September ). R103 - GENERAL REQUIREMENTS: PROFICIENCY TESTING FOR ISO/IEC 17025 LABORATORIES. American Association for Laboratory Accreditation.

American Society for Quality. (2012, Sept 12). *Total Quality Management Overview*. Retrieved from American Society for Quality: http://asq.org/learn-about-quality/total-quality-management/overview/overview.html

Amoo, P., & Thomson, N. (2009, May 28). *APCO eCrime Strategy.* Retrieved from http://www.xact.org.uk/information/downloads/internet/Ecrime_Strategy.pdf

Anderson, J. C., Rungtusanatham, M., Schroeder, R. G., & Devaraj, a. S. (1995). A Path Analytic Model of a Theory of Quality Management Underlying the Deming Management Method: Preliminary Empirical Findings. *Journal of the Decision Sciences Institute, Vol 25, Issue 5*, 637–658.

APCO. (2012). Good Practice Guide for Digital Evidence. *Good Practice Guide for Digital Evidence*. United Kingdom: Association Of Police Commissioners. Retrieved Mar 27, 2013, from http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf

APCO, A. o. (2013). *Good Practice Guide for Computer-Based Electronic Evidence.* Retrieved Feb 27, 2013, from http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf

ASCLD/LAB. (2012). *Programs of Accreditation*. Retrieved March 1, 2012, from The American Society of Crime Laboratory Directors/Laboratory Accreditation Board (ASCLD/LAB): http://www.ascld-lab.org/programs/prgrams_of_accreditation_index.html

ASCLD/LAB. (2014). *AL-PD-1020_Proficiency_Testing__Review_Program_v1.0.* ASCLD/LAB. Retrieved 08 08, 2014, from http://www.ascld-lab.org/wp-content/uploads/2014/07/AL-PD-1010_Proficiency_Test_Provider_Program_v3.0_unmked.pdf

ASCLD/LAB. (2015, February ). *Voluntary Withdrawal*. Retrieved from ASCDL/LAB: http://www.ascld-lab.org/voluntary-withdrawal/

Bacon, F. (1620). *Novum Organum.* Oxford.

Baryamureeba, V., & Tushabe, F. (2004). The Enhanced Digital Investigation Process Model. *Proceeding of Digital Forensic Research Workshop.* Baltimore, MD.

Beebe. (2009). Digital Forensic Research: The Good, the Bad and the Unaddressed. *IFIP Advances in Information and Communication Technology Volume 306 - Advances in Digital Forensics V*, 17-36.

Beebe, N. l., & Clark, J. G. (2004). A Hierarchical, Objectives-Based Framework for the Digital Investigations Process. *Proceedings of Digital Forensics Research Workshop.* Baltimore, MD.

Bill Curtis, B. H. (July 2009 ). *People Capability Maturity Model (P-CMM) Version 2.0, Second Edition.* Software Engineering Institute.

Brezinski, K. a. (2002, Feb). Guidelines for Evidence Collection and Archiving. *RFC 3227.*

Brill, A., & Pollitt, M. (2006). The evolution of computer forensic best practices: an update on orgrams and publications. *Journal of Digital Forensics Practice*, *1*, 3-11.

Business Dictionary. (n.d.). *Quality Planning*. Retrieved from Business Dictionary: http://www.businessdictionary.com/definition/quality-planning.html

Carrier, B., & Spafford, E. H. (2003). Getting Physical with the Digital Investigation Process. *International Journal of Digital Evidence*.

Carrier, B., & Spafford, E. H.-b. (2004). An Event-based Digital Forensic Investigation Framework. *Proceedings of Digital Forensics Research Workshop.* Baltimore, MD.

Casey E. (2004). Digital arms race, The need for speed. *Digital Investigation Journal*.

Casey, Eoghan. (2004). *Digital Evidence and Computer Crime, Second Edition.* Elsevier, ISBN 0-12-163104-4.

Cellebrite. (n.d.). *Mobile Lifecycle Support Center - Downlaod Generic Supported Device List*. Retrieved from Cellebrite: http://support.cellebrite.org/cellebritedesktop/PhonesList_desktop.xls

CFTT. (2013, Mar). *CFTT Methodology Overview*. Retrieved 1 7, 2013, from CFTT: http://www.cftt.nist.gov/

Ciardhuain, S. O. (2004). An Extended Model of Cybercrime Investigations. *International Journal of Digital Evidence*.

Collaborative Testing Services. (2015, April 24). *Digital & Multimedia Evidence*. Retrieved from Collaborative Testing Services: http://www.ctsforensics.com/5550-Mobile-Digital-Evidence.aspx?DepartmentId=84

Committee on the Judiciary House of Representatives. (2010). *Federal Rules of Evidence.* Washington, DC: US Govt Printing Office.

Crosby, P. (1979). *Quality is Free. New York: New American Library.* New York: New American Library.

Curtis, B. H. (July 2009). *People Capability Maturity Model (P-CMM) Version 2.0, Second Edition.* Software Engineering Institute.

Curtis, B., Hefley, W., & Miller, H. (2010). *People CMM: A Framework for Human Capital Management - Second Edition.* Pearson Education.

Curtis, B., Hefley, W., & Miller, S. (2002). *The People Capability Maturity Model: Guidelines for Improving the Workforce.* Reading, MA: Addison Wesley Longman.

Dampier, & Tanner. (2010). An Approach for Managing Knowledge in Digital Forensics Examinations. *International Journal of Computer-Science. Security, Vol. 4, #. 5*.

Dampier, T. (2010). An Approach for Managing Knowledge in Digital Forensics Examinations. *International Journal for Computer Science Security, Vol 4 # 5*.

Deming, W. E. (2000). *Out of the crisis.* Cambridge, Mass: MIT Press . ISBN 0262541157.

DFRW. (2001). DFRW Forenisc Model. DFRW.

Digital Forensic Research Workshop. (2001). Research Road Map. (pp. http://www.dfrws.org/2001/dfrws-rm-final.pdf). New York: DFRWS.

Dolin, T. (2015, June 5). Retrieved from American Society of Crime Laboratory Directors / Laboratory Accreditation Board: http://www.ascld-lab.org/ascldlab-recognizes-isoiec-17043-accreditation-of-proficiency-test-providers/

Doran, G. T. ( 1981). There's a S.M.A.R.T. way to write management's goals and objectives. *Management Review, Volume 70, Issue 11(AMA FORUM)*, 35-36.

EC-Council. (n.d.). *EC-Council website and information.* Retrieved December 12, 2011, from EC-Council website and information: http://www.eccouncil.org

*EnCE® Certification Program*. (n.d.). Retrieved 2013, from EnCase Certified Examiner (EnCE) Requirements and Process.

EU Parliament. (2004, April 29). *REGULATION (EC) No 882/2004 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 29 April 2004.* (O. J. Union, Ed.) Retrieved July 1, 2012, from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:165:0001:0141:EN:PDF

Executive Brief. (2009, Sept ). *Why is People Capability Maturity Model Necessary?* Retrieved from Executive Brief: http://www.executivebrief.com/blogs/people-capability-maturity-model-necessary/

FBI. (n.d.). *A History of the FBI*. Retrieved from The Federal Bureau of Investigation: http://www.fbi.gov/about-us/history/brief-history

Forensic Focus. (2013, Nov 15). *ISO 17025*. Retrieved from Forensic Focus: http://www.forensicfocus.com/Forums/viewtopic/p=6570941/

Freiling, F. C., & Schwittay, B. (2007). A Common Process Model for Incident Response and Computer Forensics. *Proceedings of Conference on IT Incident Management and IT Forensics.* Germany.

GIAC. (n.d.). *Security Certifications: Forensics*. Retrieved from General Information Assurance Certification: http://www.giac.org/certifications/forensics

Goodison, S. E., Davis, R. C., & Jackson, B. A. (2014). *Digital Evidence and US Justice System:* . National Institute of Justice (NIJ).

Grundy, B. (2004, January). The Law Enforcement and Forensic Examiner Introduction to Linux: A Beginner's Guide. Retrieved from www.linux-forensics.com/linuxintro-LEFE-2.0.5.pdf

Harold F. Tipton, M. K. (2007). *Information Security Management Handbook, Sixth Edition.* Auerbach Publications.

Heiser, K. (2002).*Computer Forensics: Incident Response Essentials*. Boston: Addison-Wesley.

Home Office. (2010, March). *Cyber Crime Strategy.* Retrieved from .GOV.UK: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/228826/7842.pdf

Humphrey, A. (2005). "SWOT Analysis for Management Consulting". *SRI Alumni Newsletter*.

Humphrey, W. (1989). *Managing the Software Process.* SEI.

Humphrey, W. S. (1987). *Characterizing the Software Process - A Maturity Framework.* Software Engineering Institute.

Information Technology Infrastructure Library. (2012, February 12 ). *Main*. Retrieved from ITIL Official SIte: http://www.itil-officialsite.com/

International Standards Organisation (ISO). (2012, October 15). ISO/IEC 27037:2012 Guidelines for identification, collection, acquisition and preservation of digital evidence. International Standards Organisation (ISO).

Irons, D. A. (2007). Professionalism in Computer Forensics. In A. B. Sutherland, *EC2ND 2006* (pp. Section II, Pages 115-125). Faculty of Advanced Technology, University of Glamorgan, Wales, UK: Springer London.

ISFCE. (n.d.). *Certified Computer Examiner (CCE)*. Retrieved December 10, 2011, from International Society of Forensic Computer Examiners: http://www.isfce.com/

ISO/IEC: 17025:2005. (n.d.). *ISO/IEC 17025:2005.* Retrieved January 15, 2012, from International Organization for Standardization: http://www.iso.org/iso/catalogue_detail.htm?csnumber=39883

Justice, U. D. (2004, April). Forensic Examination of Digital Evidence:. 810 Seventh Street N.W., Washington, DC 20531, USA.

Justice, U. D. (2004). *The National Criminal Justice Reference Service (NCJRS).* Retrieved February 27, 2013, from The National Criminal Justice Reference Service (NCJRS): https://www.ncjrs.gov/pdffiles1/nij/199408.pdf

K.Rogers, M., Goldman, J., Mislan, R., Wedge, T., & Debrota, S. (2006). Computer Forensics Field Triage Process Model. *Proceedings of Conference on Digital Forensics, Security and Law.*, (pp. 27-40).

Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). *Guide to Integrating Forensic Techniques into Incident Response.* Gaithersburg, Maryland.: National Institute of Standards and Technology.

Kerrigan, M. (2013). A capability maturity model for digital investigations. *Digital Investigation: The International Journal of Digital Forensics & Incident Response,Volume 10, Issue 1,(pp. 19-33).*

Kessler, G. C. (2011). Judges' Awareness, Understanding, and Application of Digital Evidence. *Journal of Digital Forensics, Security & Law, Vol. 6*(Issue 1), p55-72. 18p. Retrieved 5 7, 2012, from file:///C:/DF-C%C2%B2M%C2%B2/DF-C%C2%B2M%C2%B2%20-%20Thesis/Chapter_1/kessler_judges&de.pdf

Kohlegger, M., Ronald, M., & Stefan, T. (2009). Understanding Maturity Models - Results of a Structured Content Analysis. *Proceedings of I-KNOW '09 and I-SEMANTICS '09.* Graz, Austria.

Kohn, M., Eloff, J., & Oliver, M. (2006). Framework for a Digital Forenisc Investigation. *Proceedings of Information Security South Africa (ISSA) 2006 from Insight to Foresight Conference.* South Africa.

Kozushko, H. (2003, November 7). *Digital Evidence.* Retrieved March 10,2013,from http://infohost.nmt.edu/~sfs/Students/HarleyKozushko/Papers/DigitalEvidencePaper.pdf

Krause, J. (2010, August 31). *Computer Forensics Experts, Who's Your Daddy?* Retrieved December 8, 2011, from LAW.COM: http://www.law.com/jsp/article.jsp?id=1202471294324&rss=newswire&slreturn=1&hbxlogin=1

Krutz, R. (2006). *US Patent No. 2006/0069540 A1*. US.

Law Reform Commission. (2009). *Consultation Paper: Documentary and Electronic Evidence.* Dublin: Law Reform Commision. Retrieved from http://www.lawreform.ie/_fileupload/consultation%20papers/cpDocumentaryandElectronicEvidence.pdf

Lindsey, T. (2006). Challenges in Digital Forensics. *Presentation*. US: DFRWS.

M.Pollitt, M. (1995). Computer Forensics: an Approach to Evidence in Cyberspace. *National Information Systems Security Conference*, (pp. 487-491). Baltimore,MD.

Madeiros, J. (2011, February 13). *Computer Forensics Degrees In Demand As US Seeks Cyber Attackers*. Retrieved December 8, 2011, from Criminal Justice Degree Schools: http://www.criminaljusticedegreeschools.com/computer-forensic-degree-is-in-demand-as-us-seeks-cyber-attackers-0213111/

Mark Paulk, Bill Curtis, Mary Beth Chrissis, Charles Weber. (1993). *Capability Maturity Model for Software v1.1.* SEI. Retrieved 03 24, 2013, from http://www.sei.cmu.edu/reports/93tr024.pdf

McKemmish, R. (1999, June). What is Forensic Computing? *118*. Australian Institute o Criminology Trends and Issues. Retrieved from www.aic.gov.au/publications/tandi/tandi118.html

Michael Kohlegger, R. M. (2009). Understanding Maturity Models - Results of a Structured Content Analysis. *Proceedings of I-KNOW '09 and I-SEMANTICS '09.* Graz, Austria.

Moullin, M. (2002). *Delivering Excellence in Health and Social Care.* Buckingham: Open Univeristy.

Murphy, E., & Hands, D. (2012). Wisdom of the Crowd: How Participatory Design has evolved Design Briefing - See more at: http://www.svid.se/Research/Design-Research-Journal/Research-articles/Forskningsartiklar-2012/Wisdom-of-the-Crowd-How-Participatory-Design-has-evolved-Design-Briefing. *Swedish Design Research Journal, 2 (12)*, 28-37.

Neely, A. A. (2002). *The Performance Prism: The Scorecard for Measuring and Managing Stakeholder Relationships.* London: Financial Times/Prentice Hal.

NIJ. (2002). Results from Tools and Technologies Working Group. *Goverors Summit on Cybercrime and Cyberterrorism.* Princeton NJ.

NIJ. (2004). *Forensic Examination of Digital Evidence: A Guide for Law Enforcement.* Washington: Department of Justice - National Institute o Justice. Retrieved 3 27, 2013, from https://www.ncjrs.gov/pdffiles1/nij/199408.pdf

NIJ. (2012, Jan). *Welcome*. Retrieved from Computer Forensic Tool Testing: http://www.cftt.nist.gov/

NIST. (2004). *The National Criminal Justice Reference Service (NCJRS).* Retrieved February 27, 2013, from The National Criminal Justice Reference Service (NCJRS): https://www.ncjrs.gov/pdffiles1/nij/199408.pdf

Noblett, M. G., Pollitt, M. M., & Presley, L. A. (2000, October). *Recovering and Examining Computer Forensic Evidence*. Retrieved from The Federal Bureau of Investiggations: https://www.fbi.gov/about-us/lab/forensic-science-communications/fsc/oct2000/index.htm/computer.htm

Nuseibeh, B., & Easterbrook, S. (2000). Requirements Engineering: A Roadmap. *Paper presented at the ICSE-2000 International Conference on Software Engineering.*

Omychund v Barker , ER 15, 33 (1745).

Palmer, G. (2001). *A Road map for Digital Forensic Research.* Utica, New York: The Digital Forensics Research Working Group.

Pamplin, D. C. (2009, April 3). *The UK Register of Expert Witnesses.* Retrieved January 14, 2012, from The UK Register of Expert Witnesses: http://www.jspubs.com/downloads/PDFs/UKREW_FSR_Apr09.pdf

Paulk, Curtis, Chrissis, Weber. (1993). *Capability Maturity Model for Software v1.1.* SEI. Retrieved 03 24, 2013, from http://www.sei.cmu.edu/reports/93tr024.pdf

Peffers, K., Tuunanen, T., Gengler, C., Rossi, M., Hui, W., Virtanen, V., & al., e. (2006). The Design Science research process: a model for producing and presenting information systems research. *Paper presented at the First International Conference on Design Science Research in Information Systems and Technology (DESRIST 2006).* Claremont, CA.

Pollitt, M. M. (2003). *Who is SWGDE and what is the history?* Retrieved from SWGDE.

Reith, M., Carr, C., & Gunsch, G. (2002). An Examination of Digital Forensic Models. *International Journal Digital Evidence*.

Rick, A., Sam, B., & Jansen, W. (2014). *Guidelines on Mobile Device Forensics.* National Institute of Standards and Technology, U.S. Department of Commerce. National Institute of Standards and Technology. Retrieved 06 17, 2014, from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf

Rogers, M., Goldman, J., Mislan, R., Wedge, T., & Debrota, S. (2006). Computer Forensics Field Triage Process Model. *Proceedings of Conference on Digital Forensics, Security and Law.*, (pp. 27-40).

Sanders, E. a. (2008). Co-creation and the new landscapes of design. *CoDesign Vol 4(1)*, 5-18.

SANS. (n.d.). *SANS Institute website and information.* Retrieved January 12, 2012, from SANS Institute website and information: http://www.sans.org

SEI. (1993, Feb). Capability Muturity Model for Software. Software Engineering Institute (SEI).

Sinclair & Zairi. (1995). Effective process management through performance measurement: part I – applications of total quality-based performance measurement. *Business Process Management Journal, Vol 1 Issue 1*, 75 - 88.

Spafford, E. (2001 ). Big Computer Forensics Challenges. *DFRW*.

Srinivasan, S., & Murthy, M. (n.d.). *Process Maturity Model Can Help Give a Business an Edge.* Retrieved from iSixSigma: https://www.isixsigma.com/methodology/business-process-management-bpm/process-maturity-model-can-help-give-business-edge/

State vs. Bradley Graham Cooper, NO. COA12-926 (Supreme Court of North Carolina October 8, 2008).

State of Florida v. Casey Marie Anthony , 48-2008-CF-015606-O (District Court of Florida October 14, 2008).

Stephenson, P. (2003). *A Comprehensive Approach to Digital Incident Investigation - Elsevier Information Security Technical Report.* Elsevier Advanced Technology.

SWGDE. (2014, Feb). *Documents/Current*. Retrieved from SWGDE: https://www.swgde.org/documents/Current%20Documents

Thompson, S. P. (1910). The Life of Lord Kelvin. *Popular Lectures Vol. I*, 73.

Tipton, H., & Krause, M. (2007). *Information Security Management Handbook, Sixth Edition.* Auerbach Publications.

Verbrugge, B. (2014, March 14). *Best Practice, Model, Framework, Method, Guidance, Standard: towards a consistent use of terminology.* Retrieved from Van Haren Publishing: http://www.vanharen.net/blog/van-haren-publishing/best-practice-model-framework-method-guidance-standard-towards-consistent-use-terminology/

Winter, A. (2012, June). *The cheap all-terrain wheelchair.* Retrieved from TED: http://www.ted.com/talks/amos_winter_the_cheap_all_terrain_wheelchair?quote=1965