Standardization Requirements for Digital Forensic Laboratories: A Document Analysis and Guideline

Abdullah Khaled S Alshebel

A thesis submitted to Auckland University of Technology (AUT) in partial fulfilment of the requirements for the

Degree of Master of Computer and Information Sciences (MCIS).

School of Engineering, Computer and Mathematical Sciences

Faculty of Design & Creative Technologies

Auckland, New Zealand

2020

Declaration

I hereby declare that this submission is my own work and that, to the best of my knowledge and belief, it contains no material previously published or written by another person nor material which to a substantial extent has been accepted for the qualification of any other degree or diploma of a University or other institution of higher learning, except where due acknowledgement is made in the acknowledgements.

.....

Abdullah Khaled S Alshebel

Acknowledgements

I wish to express my deepest gratitude to my father "Dr. Khaled Alshebel", my mother "Amal Alsaeed", and my wife "Arwa Alsulaim" for their unlimited support to me during my journey through my Master's degree. The journey of writing a thesis, with the support of my supervisor Dr. Brian Cusack, was nothing but an incredible experience to me. I cannot thank Dr. Cusack enough for his dedication and support; his advice and encouragement to complete my thesis.

In addition, I wish to express my deepest gratitude to the Technical and Vocational Training Corporation (TVTC) in Saudi Arabia for sponsoring my scholarship, and my special regards to the Saudi Arabian Cultural Mission (SACM) in New Zealand for their facilitating my studies. Lastly, I wish to show my gratitude to the experts, who participated in the evaluation of the draft Standard in my thesis; their valuable time and effort is appreciated.

Abstract

In recent years, the rapid growth in technology has played an essential role in transforming the lives of humans. It has changed the way individuals communicate and it can improve their quality of life. The increase of the usage of technological solutions has led to an increase in crimes committed using technology or technologies that are present at a crime scene and have evidence. The justice systems worldwide tend to prosecute criminal actions based on evidence, and today much of the evidence is in digital formats. Digital evidence can be examined and analysed using specialized equipment and software within a digital forensic laboratory. Digital forensic laboratories control the quality and competency of the digital forensic work through the adoption of International Standards for best practice. At present there is no one Standard for Digital Forensic laboratories but rather general laboratory Standards and specialist laboratory Standards, such as medical.

Researchers have referred to in the literature, the absence of a specific digital forensics laboratory Standard, and yet after a decade, the absence remains the same. The ISO/IEC 17025, is a general Standard for the competence of testing and calibration in laboratories, and has been adapted to accredit digital forensics laboratories. However, the ISO/IEC 17025 only addresses a restricted set of risks while leaving many matters in relation to digital evidence untreated. Even though there is a paucity of literature examining digital forensic laboratory requirements, the establishment of secure practices for a new digital forensic laboratory requires a strenuous of effort. The exception is Watson & Jones (2019), which clarifies the requirements for best practices. The next step is to establish an International agreement through Standardization.

Thus, to fill this gap, this research aimed to draft a Standard proposal and implementation guideline. Design Science (DS) is chosen as the appropriate research methodology, so that a solution can be proposed but then improved by expert feedback. The draft Standard is first constructed from literature, and then improved by expert

feedback. A systematic literature review has been used through the adoption of a well-known literature search method called Preferred Reporting Items for Systematic reviews and Meta-Analyses (PRISMA). The result is that electronic libraries have been systematically searched and the selected literature used as the basis for a theoretical solution to the problem of a Digital Forensic Laboratory Standard.

The significant results from the research are the writing of a draft Standard and an implementation guideline (see Figures 5.1 and 5.2 for element analysis). The draft Standard, was termed the artefact in the design science methodology. A significant finding during the experts' evaluation of the artefact were the requirements for preparatory handling of evidence, and a requirement to establish a research centre within the digital forensic laboratory. The second concern is to assure the continuous improvement of the digital forensic laboratory technical capability and to keep ahead of changes in both designs and potential technology use. A well-known project management methodology is advised to implement the Standard. For future work, several recommendations are made that will lead to a more comprehensive management of risks around digital evidence.

Keywords: Digital forensics laboratories, ISO/IEC 17025, ISO/IEC 15189, ISO/IEC 27038, ISO/IEC 27041, ISO/IEC 27042, Digital forensic, ISO/IEC 27043, ISO/IEC 27050, Digital forensic investigation, ISO 22301, ISO/IEC 27001, ISO/IEC 27037, ISO/IEC 24775-1, ISO/IEC 24775-8, ISO/IEC 27040, Digital evidence, quality management system.

Table of Contents

List of Figures

List of Tables

List of abbreviations

AES	Audio Engineering Society
AUTEC	Auckland University of Technology Ethics Committee
BCM	Business Continuity Management
BSI	British Standards Institution
CASCO	ISO'S Committee on Conformity Assessment
CDP	Continuous Data Protection
CoC	Evidence Chain of Custody
DFS	Digital Forensics System
DS	Design Science
EA	Enterprise Architecture
EC	Engineering Cycle
EM	Evidence Manager
ESI	Electronically Stored Information
ICT	Information and Communication Technology
IEEE	Institute of Electrical and Electronics Engineers
ILAC	International Laboratory Accreditation Cooperation
IS	Information System
ISO	International Organization for Standardization
IT	Information Technology
IT DR	Information Technology Disaster Recovery
ITSM	Information Technology Service Management
KEDB	Knowledge Known Error Database
MRA	Mutual Recognition Arrangement
NGO	Non-Governmental Organization
NSBs	National Standard Bodies

OM	Operation Manual
PM	Project Manager
PMBOK	Project Management Body of Knowledge
PMI	Project Management Institute
PPM	Project Management Methodology
PRISMA	Preferred Reporting Items for Systematic reviews and Meta Analyses
QM	Quality Manual
QMS	Quality Management Systems
QUOROM	Quality of Reporting of Meta-analyses
RAID	Redundant Array of Independent Disks
RAM	Responsibility Assignment Matrix
RFP	Request for Proposal
SDOs	Standards Development Organizations
SEMI	Semiconductor Equipment and Materials International
SLA	Service Level Agreement
SNV	Schweizerische Normen-Vereinigung (Swiss Association for Standardization)
SOW	Scope of Work
TCs	Technical Committees
TM	Technical Manual
TRM	Training Manual
UN	United Nations

Chapter 1: Introduction

1.0 THE BACKGROUND, CONTEXT, AND MOTIVATION OF THE RESEARCH

In recent years, the rapid growth in information technology has played an essential role in transforming the lives of humans. It has changed the way individuals communicate and interact. The rapid growth has transformed business to be managed through technological solutions and delivered to customers through the internet. Because of the increase in the utilization of technology, it is expected the number of criminal actions using technology will also increase. Consequently, information technologies are commonly found associated with crime, and a facilitator for criminal actions such as theft, bullying, blackmail, willful damage, and so on. Mobile devices such as Smart Phones are commonly involved.

Digital evidence has a unique nature since it can be manipulated easily, and remotely. The digital evidence potentially involved in a crime requires unique treatment during the investigation lifecycle to preserve the integrity. Digital evidence has to be identified, collected or acquired, and preserved using special processes to assure the protection. In addition, as part of the investigation lifecycle, the digital evidence has to be transported to the digital forensic laboratory securely. The laboratory then has to maintain process controls to examine and analyze, and report the information. Due to the nature of the digital evidence, evidence can be manipulated or contaminated, during the journey to the examination in the laboratory. The possibility of the contamination or manipulation of digital evidence plays an essential role during prosecution, when the integrity of the evidence is challenged.

The digital forensic lifecycle can be standardized by a network of International Standards to assure the quality of the outputs delivered to a court of law. One of the key areas of concern is consistency in digital forensic evidence examination within a laboratory. This assures correct evidence examination and accuracy of results. To standardize a digital forensics laboratory, currently, there is no specified digital forensic laboratory International Standard leaving open

untreated risks that impact the trust recipients may put in laboratory results. Researchers referred to in the literature have shown the absence of a specific digital forensics laboratory International Standard, and yet after a decade, the absence remains the same. This is the primary reason to do this research.

Nevertheless, the ISO/IEC 17025, which is a general Standard for the competence of testing and calibration laboratories, can be adapted to accredit a digital forensics laboratory. This requires expertise in the field to adjust the Standard to fit the specific requirements for handling digital evidence. In addition, other guidance is available for the implementation of best practices for laboratories, but these guidelines may not assure consistency between laboratories. When each laboratory is selecting their own choice of best practices and guidelines then a user of the services cannot be assured of the general transfer of result consistency. In a worst case, scenario two expert witnesses may give a different opinion based on the same evidence.

Thus, to fill this gap of the absence of a specified digital forensics laboratory International Standard, the thesis research is aimed to draft a Standard for best practices of quality and competency for a digital forensic laboratory. The design science (DS) methodology is employed so that a draft Standard can be constructed from literature before subjecting it to expert feedback and further improvement. The gap analysis of the current documents and the actual requirements for a standardization, targeted solutions to the identified issues. To validate the tentative artefact's ability to treat the identified problems, digital forensic experts and laboratory managers were asked to evaluate the draft Standard and provide their feedback and comments on the efficacy, validity, consistency, and completeness of the draft. The guideline reflected the challenges identified and the success factors to be considered in implementation (see Figures 5.1 and 5.2 for element analysis).

Several questions have been chosen to guide this research. The research questions are as follows:

- What are the Standardization requirements for a digital forensic laboratory?
- How useful are these Standards for improving practice?
- What elements are missing from the documents?
- What is the adequacy of the guidance available for practice?

Each of these questions guide a different area of the research, and combined

together cover the scope of the research.

1.1 THE STRUCTURE OF THE THESIS

The thesis is structured into seven chapters, where each chapter plays an essential role in the sequence of the proposed solution. This chapter presents an introduction to the thesis through description of the background, context, and motivation of the research. Chapter two will review the literature, where a common language has to be outlined regarding the Standard and its implementation. In addition, the chapter details current digital forensic Standards and general laboratory Standards. Lastly, the selected issues and problems are outlined, with the problem statement that this research aims to resolve. Chapter three presents the objectives, questions, and methods of the research. The research methodology outlines how the literature search is scoped and the methods used to produce the draft Standard.

Chapter four describes the quality and competency requirements of digital forensic laboratories. The requirements are divided into two sections: management requirements and technical requirements. Chapter five defines the proposed guideline for adopting the draft Standard, starting with the identification of the gap between the current position of the laboratory and the targeted architecture for a Scope of Work (SOW). In addition, challenges for the adoption are identified and success factors for a successful implementation.

Chapter six is the outcome of the validation stage of the research methodology, where experts have been consulted to confirm and improve the draft Standard. The chapter articulates the experts' credentials and when and how the consultation has been performed. After that, the chapter presents the primary feedback and analysis of the findings. Chapter seven gives recommendations for future research, and the conclusion to the research project.

Chapter 2: Literature Review

2.0 INTRODUCTION

This chapter is the result of a systematic literature review that been completed through the AUT library system that includes the BSI Standards database. The literature review came from a wide range of sources to cover the fundamentals of Standardisation, Standards implementation, general laboratory Standards, and the ISO digital forensic Standards. The identified gaps were analysed to select the primary concerns for a problem statement. Solutions were also outlined from the literature analysis.

2.1 STANDARDISATION

Organisations often tend to work based on Standardisation practices to control their functions. Standardisation can be defined as the process of making the same type of activities to have equal qualities ("Oxford Dictionary of English, 3 ed," 2010). In the last century, Standardisation organisations expanded their reach in many geographic locations in order to fulfil the demand for Standardisation practices. Hallstrîm (2004) point out that the establishment of Standardisation organisations during that century has increased around the whole world. The listed bodies in Table 2.1 are examples of the Standardisation organisations.

Table 2.1: Examples of the Standardisation organisations bodies.

Organisation	Year of establishment
British Standards Institution (BSI)	1901
Deutsches Institut für Normung (DIN)	1917
American National Standards Institute	1918
Schweizerische Normen-Vereinigung (SNV) (Swiss Association for Standardization)	1919
Swedish Standards Institute (SIS)	1922
Norges Standardiseringsforbund (NSF)	1923

Den Danske Standardiserings Kommission (DS)	1926
L'Association francaise de normalisation (AFNOR)	1926

Standards, in general, are classified into two different classifications: formal and informal Standards. According to Tantra (2016), formal Standards are published by official Standard entities, which are recognised by National Standard Bodies (NSBs) (163 members as retrieved on July-2019 https://www.iso.org/members.html). There are usually one per country, such as the British Standards Institution (BSI) and Schweizerische Normen-Vereinigung (SNV) (see Table 2.1), where the recognition covers regional, national, and International scopes. The three International Standardization entities are ISO, IEC, and ITU (http://www.iso.org, http://www.iec.ch, https://www.itu.int). NSBs are government recognized, but often independent entities. NSBs usually do not develop the technical content of the Standards, which is developed by Technical Committees (TCs). On the other hand, informal Standards which are published by industry or sector Standards organizations, are referred to as Standards Development Organizations (SDOs). Some SDOs are highly respected and well known, for instance, Institute of Electrical and Electronics Engineers (IEEE) (http://Standards.ieee.org/), Audio Engineering Society (AES) (www.sae.org/Standards/), Technical Association of the Pulp and Paper Industry (TAPPI) (www.tappi.org/Standards), and Semiconductor Equipment and Materials International (SEMI) (www.semi.org/Standards). The process of developing formal and informal Standards is the same, but the Standards' approval is undertaken by different entities, such as NSBs in the case of formal Standards and SDOs for informal Standards.

The International Organization for Standardization (ISO), one of the main International Standardization entities, and is a Non-Governmental Organization (NGO). It maintains affiliation with the United Nations (UN) (Murphy & Yates, 2009; Seo, 2013). ISO members are either a part of a governmental structure or an NGO. ISO develops its Standards through its TC and sub communities, with currently 246 committees (*ISO - Technical Committes*). These meet electronically through a collaborative knowledge management system for discussions in order to

collaborate for the process of Standard production and review (Riillo, 2013). Murphy and Yates (2009) observes that ISO do not regulate or legislate, and all of its work is the result of the interoperability within its committees. ISO Standards became obligatory due to the partnership of ISO and the governmental legislation within its national members. There are two types of Standards documents: *Normative and Informative*. According to Hatto (2013), *Normative* documents are the Standards which contain requirements, where organisations have to comply with the requirements for Standard certification. *Informative* documents, on the other hand, are the Standards, which do not have requirements; therefore, it cannot be complied and claimed for Standard certification.

2.2 IMPLEMENTATION

The adoption of a Standard is motivated by work benefits such as efficiency and cost savings. Also to ensure the quality, reliability and safety of the output product or service. It is thought that adopting Standards inhibits innovation, but experts argue that the Standards represent the best way of doing things, and this encourages innovators to leave the trivial matters and focus on the core of their innovation (Hatto, 2013). The cost to an organisation is the documentation, the change management and maintenance cycles, and the retirement of a Standard. According to ISO in GUIDE 2:2004, the only implementable Standard type is the normative Standard; and, there are two ways to apply a normative document: direct and non-direct. Direct application is to implement an International Standard in a national jurisdiction regardless of any other normative document. On the other hand, the indirect application is to implement an International Standard through the adoption of alternative normative documents.

2.3 DIGITAL FORENSIC STANDARDS

The absence of a Digital Forensic Laboratory Standard is currently covered by a set of interoperable Standards, where each Standard either plays a role in covering one or more of the digital forensics processes and activities or fills the missing gap in another Standard. The interoperable Standards aim to cover the digital forensics processes at multiple levels and for various areas of application. The Standards

currently cover the following areas: Information security incident management, security techniques in managing digital evidence, digital redaction, storage security, incident investigative method, digital evidence interpretation and analysis , security information and event management, investigation models, electronic discovery, and business forensic governance (Klipper, 2011). The digital evidence investigation is focused on acquiring and analysing digital evidence within a context or a jurisdiction for the organization itself to ensure the maximum beneficial impact due to the process of discovery. According to Veber and Klíma (2014), the digital evidence forensic field is emerging due to the existence of practices. The emerging ISO Standards of 27000 family play a significant role in the digital evidence analysis procedures, which is one of the primary layers for digital evidence forensics. Figure 2.1 summaries the current digital forensic Standards.

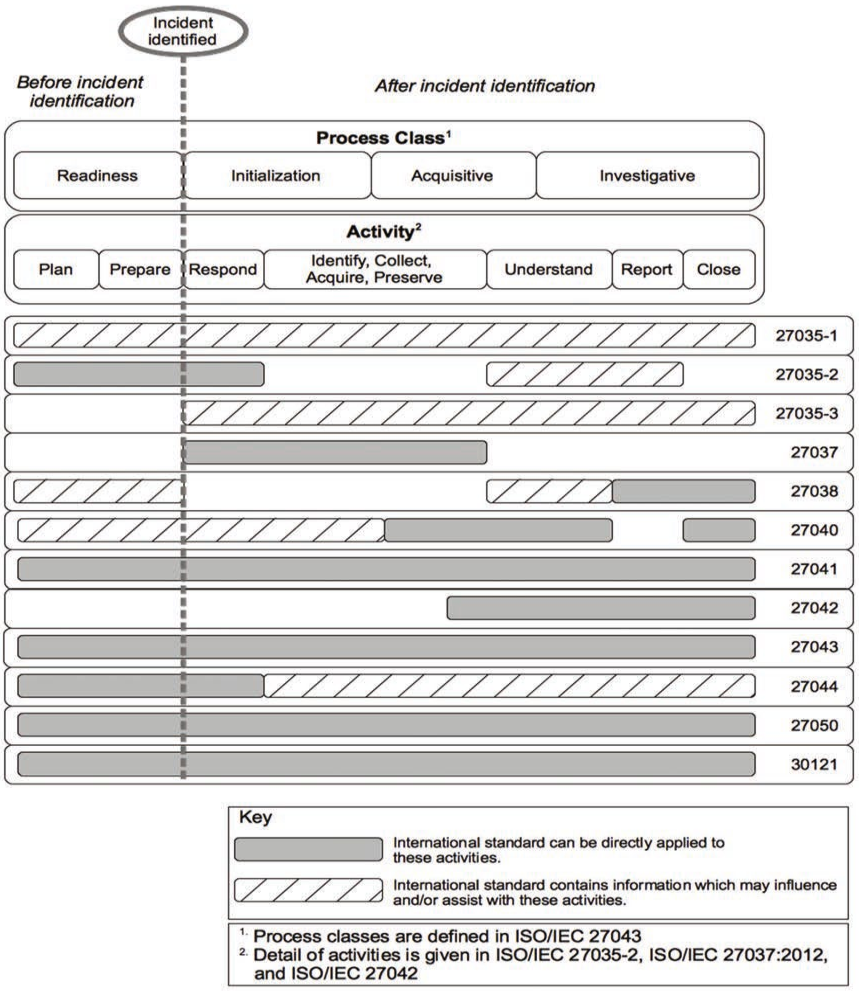


Figure 2.1: Digital Forensics process classes and activities. Reprinted from *Information technology — Security techniques Incident investigation principles and processes (BS EN ISO/IEC 27043:2016)* (p. ix), by The British Standards Institution, 2016, London, UK: BSI Standards Limited.

It is observed, in Figure 2.1, that the ISO/IEC 27000 family documents interpret digital forensics investigation as a set of processes. There are four types of processes: Readiness, Initialization, Acquisitive, and Investigative processes. The Readiness processes are responsible for the preparation of pre-incident events. This impacts the digital evidence analysis through the processes of the *ISO/IEC 27035-2:2016 "Information security incident management"*. For example, it is hard to gather the digital evidence if the IT infrastructure system does not log events during the functioning of the system (Sonntag, 2013; Veber & Klíma, 2014). International Organization for Standardization (2015a), gives the processes required to be established within the Readiness phase which can be grouped into three, as showed in Figure 2.2: Planning, implementation, and assessment.

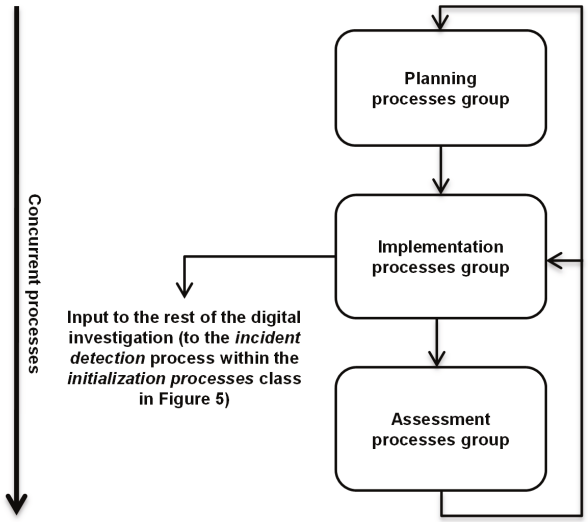


Figure 2.2: Readiness processes groups. Reprinted from *Information technology — Security techniques Incident investigation principles and processes (BS EN ISO/IEC 27043:2016)* (p. 8), by The British Standards Institution, 2016, London, UK: BSI Standards Limited.

The planning processes group includes: the process of scenario definition, the processes of potential digital evidence sources identification, the process of pre-incident gathering planning, the processes of storage and handling data, representing of potential digital evidence, the process of incident detection, and defining the organisation system architecture process. The implementation processes group is for the implementation of the planned activates in the planning processes group. Consequently, this group includes the implementation of the system architecture process, the process of incident detection, and the analysis of

pre-incident data representing the potential digital evidence. In addition, it handles the gathering, storage, and managing of data representing the potential digital evidence. Lastly, is the assessment processes group. This group focuses on the assessment of the implementation success in the previous processes group. This group contains the assessment of the implementation process and implementation results. The interaction and activities sequence of the Readiness phase are summarised in Figure 2.3.

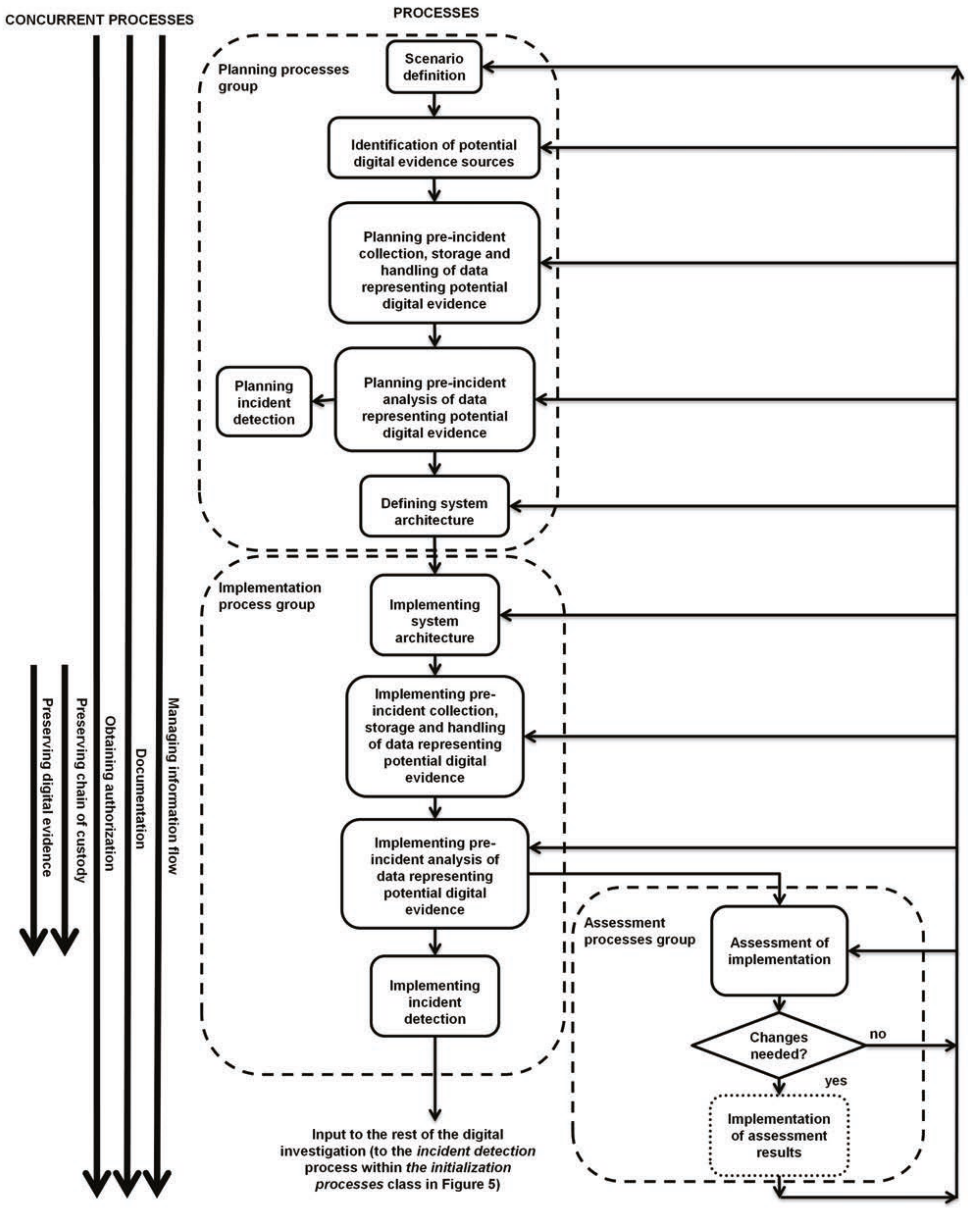


Figure 2.3: Mapped processes of the Readiness phase. Reprinted from *Information technology — Security techniques Incident investigation principles and processes (BS EN ISO/IEC 27043:2016)* (p. 10), by The British Standards Institution, 2016, London, UK: BSI Standards Limited.

The initialisation processes are a set of activities connected to the incident and start an investigation. This phase initialises the digital investigation by detecting the incident, and the first response to that occurrence along with the preparation for the remainder of the incident investigation processes. Usually, this part of the digital forensic lifecycle is done through the processes of *ISO/IEC 27035-2* and *ISO/IEC 27037 "Guidelines for identification, collection, acquisition and preservation of digital evidence"* (Veber & Klíma, 2014). According to International Organization for Standardization (2015a), this phase includes the following processes: incident detection, first response, planning and designing what and how to get the required information, and deciding which tool(s) and techniques suits a case. Planning and preparing for the investigation include where the investigators start to encounter the crime scenes and establish a strategic plan to handle this investigation. Thus, all the investigation tasks (what, why, who, how, and when) must be clarified during this step, which would impact the success of the investigation. The mapped processes of the initialization phase are in Figure 2.4.

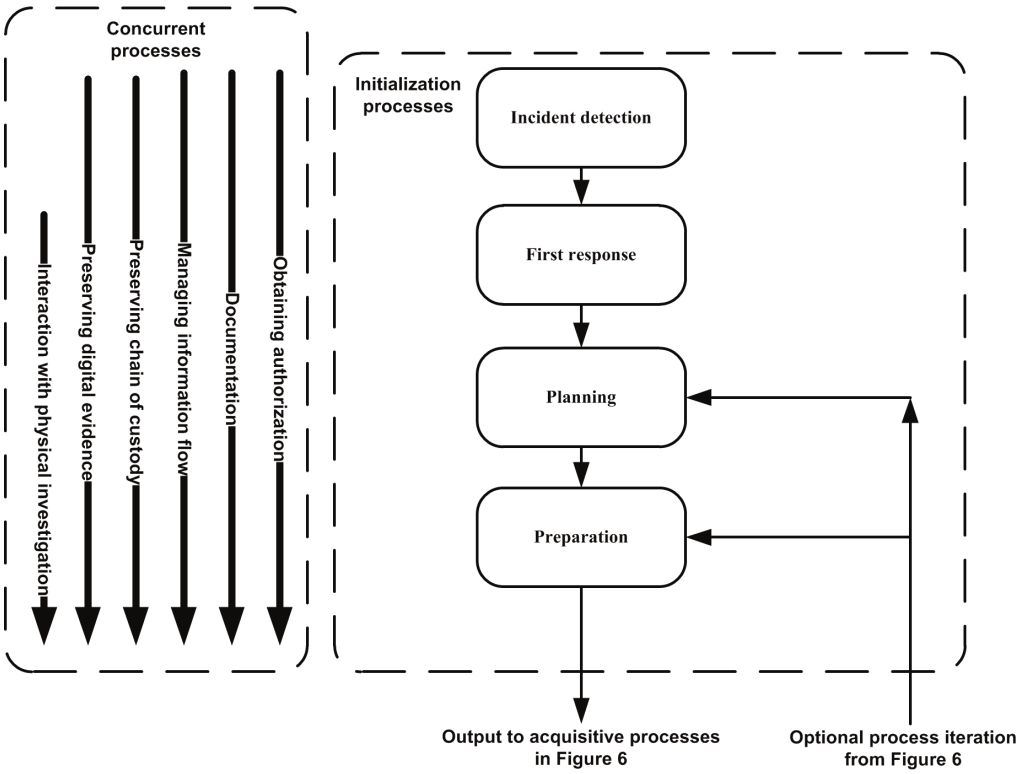


Figure 2.4: Mapped processes of the Initialization phase. Reprinted from *Information technology — Security techniques Incident investigation principles and processes (BS EN ISO/IEC 27043:2016)* (p. 14), by The British Standards Institution, 2016, London, UK: BSI Standards Limited.

The acquisitive processes are a set of activities that cover identifying, collecting, transporting, and storing potential digital evidence. This part of the digital forensic lifecycle, primarily, is covered in the digital evidence Standard *ISO/IEC 27037*. The acquisitive processes consist of the identification process, collection process, transportation process, evidence acquisition (optional), and storage process for the potential digital evidence. The mapped processes of the acquisitive phase are in Figure 2.5.

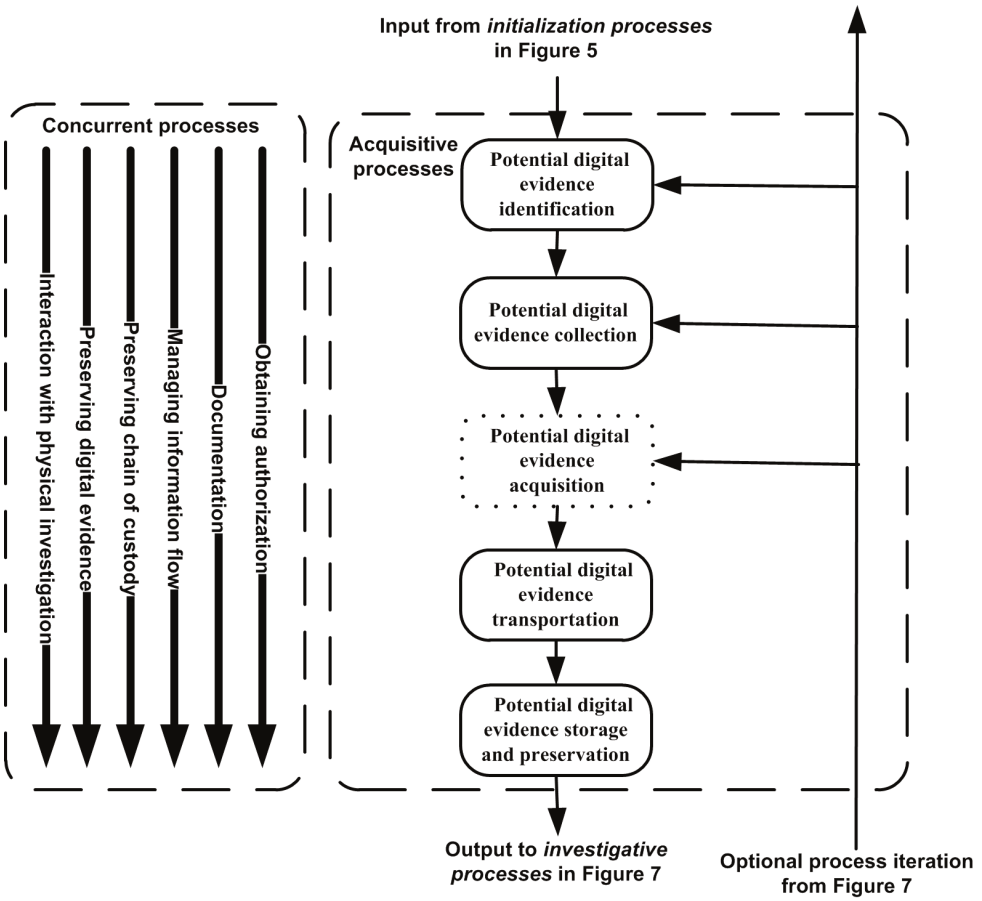


Figure 2.5: Mapped processes of the Acquisitive phase. Reprinted from *Information technology — Security techniques Incident investigation principles and processes (BS EN ISO/IEC 27043:2016)* (p. 16), by The British Standards Institution, 2016, London, UK: BSI Standards Limited.

Lastly are the investigative processes. These processes focus on investigating the identified incident that led to a digital investigation. The activities of this phase are mainly focusing on the analysis of digital evidence and analysis. It includes the evidence interpretation and writing and presenting the digital evidence investigation report. Also, this phase contains the process of the investigation closure, where the evidence is returned (if needed) after recording the acceptance or rejection of the

investigation hypothesis(es) and recording the learned lessons. These activities are seen in Figure 2.6. This phase is primarily covered by the reference *ISO/IEC 27041 "Guidance on assuring suitability and adequacy of the incident investigative method"* and *ISO/IEC 27042 "Guidelines for the analysis and interpretation of digital evidence"*.

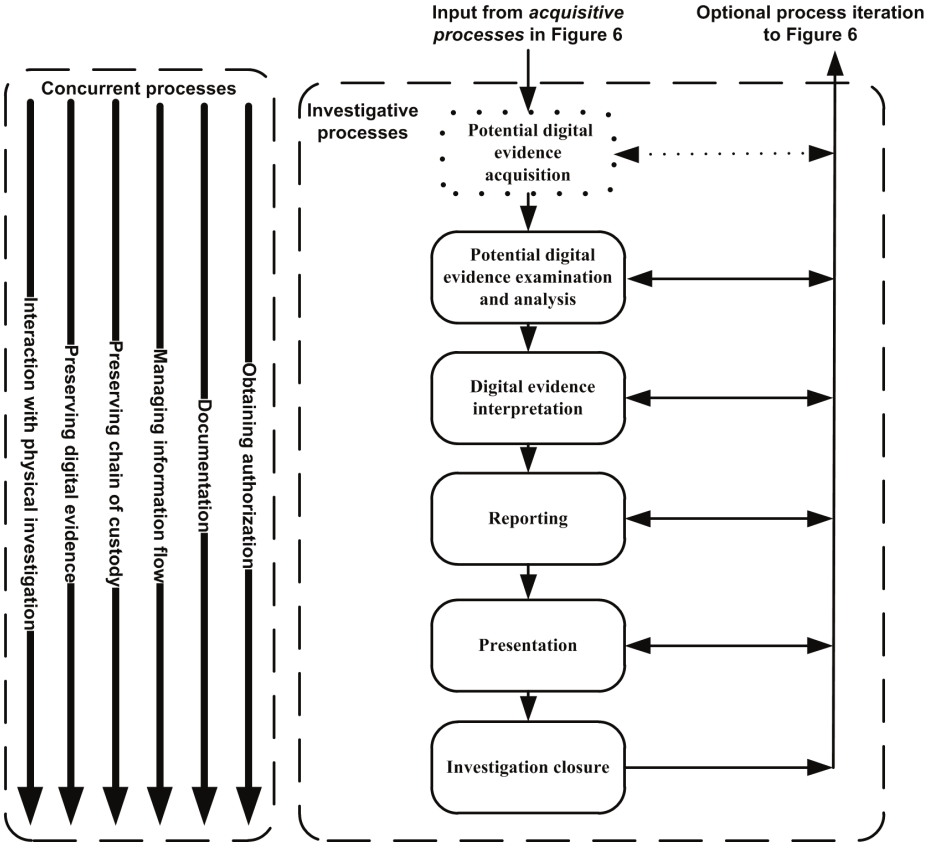


Figure 2.6: Mapped processes of the Investigative phase. Reprinted from *Information technology — Security techniques Incident investigation principles and processes (BS EN ISO/IEC 27043:2016)* (p. 18), by The British Standards Institution, 2016, London, UK: BSI Standards Limited.

In Figures 2.4, 2.5, and 2.6, there are concurrent processes working alongside the digital investigation processes classes, which converted to actionable items during the investigation to assure the full compliance of the digital evidence for a court of law. In addition to the primary Standards that carry out the process classes in Figure 2.1, there are two other types of Standards involved within the digital forensic life cycle. These are Standards work among all life cycles (*ISO/IEC 27043, ISO/IEC 27050*, and *ISO/IEC 30121*) and Standards, which contribute a small amount within each process, class (*ISO/IEC 27038* and *ISO/IEC 27040*). The *ISO/IEC 27043 "Incident investigation principles and processes"* contain five processes:

identification, collection, examination, analysis and presentation. Each works within ten activities and all the four phases of the digital forensics lifecycle, as shown in Figure 2.1, which maps the digital forensics processes and activities (Kao, Chao, Tsai, & Huang, 2018).

Unlike the ISO/IEC 27043, the ISO/IEC 27050 "Electronic discovery" contributes within the digital forensic life cycle as a three-part Standard: *ISO/IEC 27050-1:2016 "Overview and concepts of the Electronic discovery"*, *ISO/IEC 27050-2:2018 "Guidance for governance and management of electronic discovery"*, and *ISO/IEC 27050-3:2017 "Code of practice for electronic discovery"*. It provides a legal perspective, in addition to the governance, processes, and readiness of the E-discovery system. It is not designed to contradict or/and supersede with any local jurisdiction system requirements but to provide a framework and checksheet for action (Hibbard, 2014). In addition, "Judges on E-Discovery: Keep It in Perspective" 2013) illustrate that this Standard would significantly contribute to solving cross-border digital investigations.

The *ISO/IEC 30121:2016 "Governance of digital forensic risk framework"* functions as a forensic readiness for businesses Standard, where the Information Technology (IT) security solutions and technologies cannot protect information assets of a corporate by itself (DATE, 2013). This Standard functions primarily pre, during, and post the occurrence of an incident, where it addresses the performance measurements for the governing body, and the relationship to the requirement of the digital forensic risk in collaboration with the incident management processes (Grobler, 2012). This Standard is interacting with the incident management processes in the pre-incident phase through to the readiness. This uses existing information from a prior incident(s) report within the Knowledge Known Error Database (KEDB) in the Information Technology Service Management (ITSM) processes (Kim, Kim, Hwang, & Yoo, 2007; Rao, Mansingh, & Osei-Bryson, 2014). The KEDB is a database containing the known errors of problems, which are the root causes of an incident(s), which have been solved previously; and, where searching for available solutions and writing the solution information are parts of the incident processes (Kim et al., 2007; Long, 2008). The ISO/IEC 27038 "Specification for digital redaction" specifies characteristics of methods and tools to perform techniques for digital reduction on digital documents (International Organization for Standardization, 2015a). This Standard can be applied directly

during the investigative processes group actions, and along with the indirect contribution before the identification of an incident involvement in a digital forensic investigation (Fal', 2017). The *ISO/IEC 27040:2015 "Storage security"* detail to businesses how to plan, design, document, and implement the risk mitigation of the data storage security and management (International Organization for Standardization, 2015b). Additionally, this Standard is guidance for originations on threat, design, and control aspects associated with security and the area of protection. This Standard can contribute indirectly before collecting the investigation data, especially during the readiness processes, but the most important contribution is the guidance of this Standard for safe deletion of the evidence (data) and the destruction of case data itself after the case is closed in court when required (International Organization for Standardization, 2015a, 2015b). To conclude the importance of the digital forensics' Standards, adopting these new Standards would improve capability to handle security mitigation along with the secure management in the post-incident phases.

2.4 GENERAL LABORATORY STANDARDS

The challenges of tailoring International Standards to meet the requirements of digital forensic laboratories, including the applicability of the ISO/IEC 17025 clauses, requires elaboration so that the issues and problems can be identified. In addition, the coverage of the requirements of digital forensic laboratories in the area of Quality Management Systems (QMS) found in serval International Standards needs clarification. A comparison of scopes and content between Standards will give the gaps and show the areas a standardisation for digital forensic laboratories should fill. Furthermore, validation of the instrumentation used for accreditation should be analysed, and the consistency between the digital forensic processes and activities evaluated. This analysis will assist the design of a new digital forensic laboratory Standard that is relevant and addresses current untreated risks.

In addition to the ten digital forensic Standards within the ISO/IEC 27000 family referenced above, there are several related Standards from another ISO group, which contribute to the forensics lab requirements. Generally, Standards can be applied via self-recognition, accreditation, or certification; where the self-recognition depends on an organisation self-assessment. Certification is the

provision of a certificate certifying that the system, product, or service met the specific requirements; also, this could be provided to a person (International Organization for Standardization). On the other hand, accreditation is the formal recognition by an organization that been recognized as an accreditation body by one of the official Standard entities. Experts, to assure the competence of an organization in a defined technical knowledge base (Competency or management system based standards, perform the recognition*? Frequently asked questions*, 2016). Laboratory accreditation is termed conformity assessment and it is performed using competency-based Standards. Most of the accreditation bodies have a strategic partnership with the International Laboratory Accreditation Cooperation (ILAC), where the ILAC is an International organisation for accreditation bodies which operates under *ISO/IEC 17011:2017 " Conformity Assessment - Requirements for accreditation bodies accrediting conformity assessment bodies"* (Wilson-Wilde, 2018). ILAC is contributing to the accreditation of the conformity assessment bodies under an arrangement called Mutual Recognition Arrangement (MRA) (International Laboratory Accreditation Cooperation (ILAC), 2015). The laboratory competency-based Standards are managed, and developed by an ISO committee called ISO's Committee on Conformity Assessment (CASCO) (International Organization for Standardization). CASCO developed three different types of laboratories Standards, which are used to accredit and confirm an organization is competent to provide a reliable service, as follows:

- **Testing laboratories**: *Through ISO/IEC 17025:2017 "General requirements for the competence of testing and calibration laboratories"*. This Standard is an applicable Standard for any testing laboratory due to the fulfilment of generic requirements; including digital forensics laboratories.

- **Medical testing laboratories**: Through *ISO 15189:2012 "Medical laboratories. Requirements for quality and competence"*. This Standard is a subset of the ISO/IEC 17025, but it focuses on the quality management systems of medical laboratories.

- **Inspection bodies**: Through *ISO/IEC 17020:2012 "Conformity assessment. Requirements for the operation of various types of bodies performing inspection"*. This Standard contains the examination criteria for inception bodies in order to provide a certification for organizations.

In addition to the above competency-based Standards, there are other Standards that focus on the management perspective, which can be applied to the digital forensic laboratories in the use of auditing the laboratory service as follows:

- **ISO 9000 series for QMS:** *ISO 9001:2015 "Quality management systems. Requirements"*, *ISO/TS 9002:2016 "Quality management systems. Guidelines for the application of ISO 9001:2015"*, and *ISO 9003:1994 "Quality systems. Model for quality assurance in final inspection and test"*.
- **Environmental management**: *ISO 14001:2015 "Environmental management systems. Requirements with guidance for use".*

In order to improve the consistency of the digital forensic processes starting from the pre-incident phase until the case closure, all the levels of the processes have to be standardized including technical, management, and governance. One of the primary stages of the evidence investigation is the examination of evidence in the digital forensic laboratory, and an accredited laboratory can ensure that the digital forensic laboratory can produce a reliable result. In the case of digital forensics, the *ISO/IEC 17025* can be used for general laboratory accreditation. *ISO /IEC 17025* is a normative reference specifying the general requirements for the competence of the laboratory's operation. This Standard is applicable for laboratories and laboratory activities. The Standard guides laboratories involved in forensic analysis and examination using various types of testing methods: Standard, non-Standard, and laboratory-developed (Guo & Hou, 2018; Sommer, 2018). There have been three versions of *ISO/IEC 17025*: 1999, 2005, and 2017. The significant improvement between the 1999 version and 2005 is that the requirement for commitment and responsibility from top management to the continuous improvement of the management system, along with the focus on the relationship with the customer including the communication mechanism. This is aligned with *ISO 9001:2000 "Quality management systems. Requirements"*. According to International Organization for Standardization (2017), the ISO/IEC 17025:2017

consist of the following clauses:

- **General requirements:** Where it covers the impartiality and confidentiality of the laboratory.

- **Structural requirements:** This clause covers the legal identification of the laboratory along with the clear identification of the laboratory activities and responsibility. It has to clarify the laboratory hierarchy and the responsibilities and authorities for the employees (technical and service support) and the management. Also the relationship between the organisation internal entities to ensure the effectiveness of the laboratory activities.

- **Resource requirements:** This covers in-depth the availability of the internal and external resources such as facilities, personnel, lab equipment, system, and the defined support services that are necessary to perform the defined laboratory activity scope.

- **Process requirements:** This clause covers the entire laboratory life cycle processes, including the review of the contracts, tenders, and requests. In addition, it extends to the selection, verification, and validation of the testing methods along with sampling and handling the tests. Furthermore, it addresses the importance of the technical laboratory records and the measurement of uncertainty evaluation. This section also focuses on the processes of the validity of results, reporting a result, and handling customer complaints. Moreover, it specifies the requirement of the laboratory in controlling data and information management.

- **Management system requirements:** This clause covers the requirements of establishment, documentation, implementation, and maintenance of the laboratory management system, which ensures the quality of the laboratory results. This management system should be capable of supporting the

requirement of the above clauses, as the implementation of the above clauses in this system is mandatory.

Marshall and Paige (2018) report in their study that the first edition of the ISO/IEC 17025 has eight principles, which are covered within the Standard. All of these principles have been retained in both the 2005 and 2017 versions. The eight principles are listed as follows:

- **Capacity:** The concept covers that the laboratory must have sufficient resources (the skilled and knowledgeable people to perform the assigned task, the required equipment and facilities, the quality control management, and the proper processes) in order to undertake the work order.

- **Exercise of responsibility:** This principle articulates that each person has a delegated authority to execute a function that contributes to completing an activity, and the organisation can demonstrate accountability thought the test result.

- **Scientific method:** This principle illustrates that the undertaken work by the organisation has to be done scientifically, and within acceptable deviations. All processes need be examinable by experts in that field.

- **The objectivity of results:** This principle clarifies that:
  The testing result is primarily based on measurable or derived quantities. In addition, the tests have to be performed by a qualified person, who has recognized qualifications to do the assigned work activities.

- **Impartiality of conduct:** The testing is performed through accepted scientific approaches as the primary influence on the result and overriding the influence of the performer who executes the test, or any other influence considered secondary, and is prohibited from taking precedence.

- **Traceability of measurement:** The principle articulates that: The produced result, from the laboratory, has to be based on a recognised system management theory that derives from an accredited/recognised Information

System (IS). In addition, the comparison of measurement in the accredited/recognised devices, and the device which produces the objective result is unbroken through the whole measurement chain, including for the uncertainty result.

- **Repeatability of the test:** The objective results have to be the same when the tests are repeated, or within acceptable deviations, in the subsequent testing. In addition, this testing has to be performed by the same technician using the same equipment through the same processes and procedures.

- **The transparency of the preformed process:** The laboratory processes, which are involved in the objective result, must to be open to any internal or external security assessment, which demonstrate the effectiveness of the laboratory ability to identify and mitigate any factor that may adversely, or scientifically affect the objective results.

2.5 SUMMARY OF THE ISSUES AND PROBLEMS

The preceding sections have reviewed a relevant literature in relation to Standards and in particular literature selected in relation to digital forensic laboratories. This section completes the analysis by listing the outstanding issues and problems.

2.5.1 Analyses of the Issues and Problems

A Digital Forensics Survey (Guo & Hou, 2018), states that the use of ISO/IEC 17025 for accreditation has several reasons: International recognition for testing competence, performance benchmarking, and marketing advantage. However, the same writer stated that there have been arguments whether this Standard is the most suitable for a digital forensic laboratory especially that this Standard has become a mandatory requirement for digital forensic laboratory accreditation in the United Kingdom. For many reasons, digital forensic laboratories are opposed to the ISO/IEC 17025 due to the high cost of adoption, the impact of the inconsistent risk treatment, and the generic nature. It also requires specialist skill to implement the Standard. Although ISO/IEC 17025 is not designed especially for digital forensic

laboratories, it can be useful as a starting position for implementing controls within a digital forensic laboratory. A previous study published by Hykš and Koliš (2014) analysed the adaptability of the ISO/IEC 17025 (2005 version) to be applied directly to a digital forensic laboratory, and the result is presented in Table 2.2.

Table 2.2: The application of the ISO/IEC 17025 requirements (2005 version) on a digital forensics laboratory.

Clause number	Clause title	Application
4	Management requirements	Fully applicable
4.1	Organization Partly	Partly applicable
4.2	Management system	Fully applicable
4.3	Document control	Fully applicable
4.4	Review of requests, tenders and contracts	Fully applicable
4.5	Subcontracting of tests and calibrations	Fully applicable
4.6	Purchasing services and supplies	Fully applicable
4.7	Service to the customer	Fully applicable
4.8	Complaints and/or calibration work	Fully applicable
4.9	Control of nonconforming testing and/or calibration work	Fully applicable
4.10	Improvement	Fully applicable
4.11	Corrective action	Fully applicable
4.12	Preventive action	Fully applicable
4.13	Control of records	Fully applicable
4.14	Internal audits	Fully applicable
4.15	Management reviews	Fully applicable
5	Technical requirements	
5.1	General	Fully applicable
5.2	Personnel	Fully applicable
5.3	Accommodation and environmental conditions	Not applicable
5.4	Test and calibration methods and	Partly applicable

	method validation	
5.5	Equipment	Not applicable
5.6	Measurement traceability	Partly applicable
5.7	Sampling	Not applicable
5.8	Handling of tests and calibration items	Fully applicable
5.9	Assuring the quality of test and calibration results	Fully applicable
5.10	Reporting the results	Fully applicable

The result of the analysis of the suitability of the ISO/IEC 17025 to be applied to a digital forensics laboratory resulted in three qualified situations: clauses are fully applicable, clauses that require to be excluded, and clauses that are partly applicable. In addition, there are clauses that are not applicable to the digital forensic laboratory, but can be modified to fill a gap within the implementation such as clause 4.8 where it can be converted from complaints and/or calibration work to take over the complaints processes of digital forensics laboratory. As mentioned above, the management system clause covers the requirement of establishment, documentation, implementation, and maintenance of the laboratory management system, which ensure the quality of the laboratory results, and the system should be capable of supporting all the other clauses since the implementation of clauses within the system is mandatory. Although ISO/IEC 17025 is not designed especially for digital forensic laboratories, it can be useful as a start in the case of designing a management system. In addition, there is a widely used Standard for QMS, which is ISO 9001 (International Organization for Standardization, 2014). This Standard provides the basics requirements of an organisation management system given its nature, which can be adopted by any entity (International Organization for Standardization, 2008). The Standards structure can be seen in Table 2.3, and where its requirements from a process point of view, can be observed in Figure 2.7.

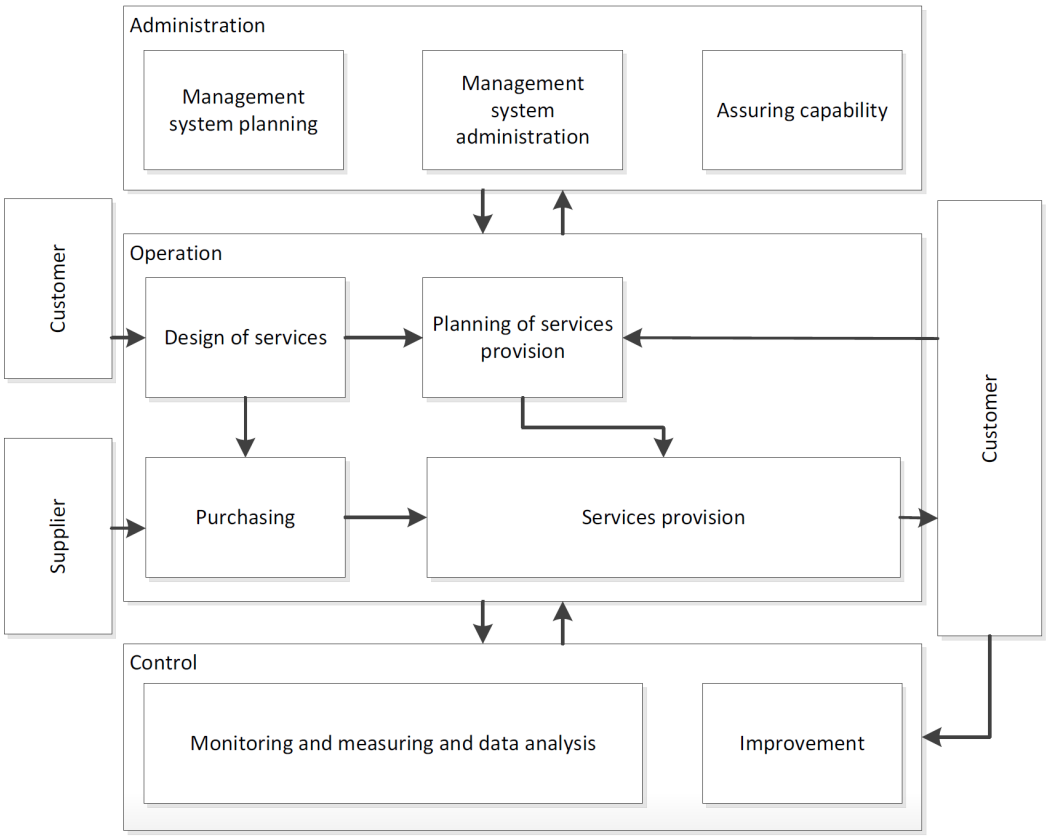


Figure 2.7: The requirements of ISO 9001 from a process point of view. Reprinted from "Development of the Digital Forensic Laboratory Management System Using ISO 9001 and ISO/IEC 17025," by Hykš, O., & Koliš, K., 2014, IDIMT 2014: Networking Societies - Cooperation and Conflict, 22nd Interdisciplinary Information Management Talks, p. 87-94.

In the case of designing a digital forensic laboratory management system, all the ISO 9001 processes are fully applicable. ISO/IEC 17025 and ISO 9001 are required to be mapped to fulfil the requirement of a digital forensic laboratory management system because neither of them covers all the aspects of the system. Hykš and Koliš (2014) in Table 2 outline a comparison of the coverage of the requirement of digital forensic laboratory management system between ISO/IEC 17025 and ISO 9001.

Table 2.3: Comparison of the Coverage of the Requirements of ISO 9001 and ISO/IEC 17025. Adopted from "Development of the Digital Forensic Laboratory Management System Using ISO 9001 and ISO/IEC 17025," by Hykš, O., & Koliš, K., 2014, IDIMT 2014: Networking Societies - Cooperation and Conflict, 22nd Interdisciplinary Information Management Talks, p. 87-94.

ISO 9001		ISO/IEC 17025	
Clause	**Requirement**	**Clause**	**Coverage of the requirement**
4.1	structure and scope of management system	4.1, 4.2	partly covered

4.2	quality manual, control of documents	4.2, 4.3, 4.12	Fully covered
5.1	assuring top management commitment	4.1, 4.2, 4.15	Fully covered
5.2	identification and fulfilment of customer requirements	4.4	Fully covered
5.3	quality policy	4.2	Fully covered
5.4	setting goals and management system planning	4.2	Fully covered
5.5	responsibility and authority, quality manager and internal communication	4.1, 4.2, 4.11	partly covered
5.6	management review	4.15	Fully covered
6.1	provision of resources	4.4, 4.7, 4.10, 5.4, 5.10	Fully covered
6.2	staff capability	4.1, 5.2, 5.5	Fully covered
6.3	infrastructure capability	4.1, 4.6, 4.12, 5.3, 5.4,5.5, 5.6, 5.8, 5.10	Fully covered
6.4	Working environment capability	5.3	Fully covered
7.1	planning of services provision	4.1, 4.2, 5.1, 5.4, 5.9	Fully covered
7.2	assuring fulfilment of customer requirements, communication with customer	4.4, 4.5, 4.7, 4.8, 5.4,5.9, 5.10	Fully covered
7.3	design of services	5.4, 5.9	partly covered
7.4	selection and evaluation of suppliers	4.6	Fully covered
7.5	control of services provision, validation of processes, identification, preservation of product	4.1, 4.6, 4.12, 5.1, 5.2, 5.4, 5.5, 5.6, 5.7, 5.8, 5.9, 5.10	partly covered
7.6	calibration and verification of measurement equipment	5.4, 5.5	Fully covered
8.1	continual improvement	4.10, 5.4, 5.9	Fully covered
8.2	monitoring and measurement, internal audit	4.5, 4.6, 4.9, 4.10, 4.11,	partly covered

		4.14, 5.5, 5.8, 5.9	
8.3	Control of nonconforming services	4.9	Fully covered
8.4	analysis of data	4.10, 5.9	Fully covered
8.5	preventive and corrective actions	4.9,4.10, 4.11, 4.12	Fully covered

In the case of partial coverage, since the ISO/IEC 17025 does not cover the whole scope of ISO 9001 requirements, it is advised that the requirements in ISO 9001 have to be used instead. On the other hand, in the case of full coverage of the requirements, ISO/IEC 17025 can be used to fulfil these requirements. It is observed that the processes of these two Standards have to be mapped to achieve management system effectiveness and efficiency. The biggest gap between the requirements of the management system within these Standards is within the requirements of the structure of an organisation, where ISO/IEC 17025 does not require a structure based on processes (Hykš & Koliš, 2014). In the case of a digital forensic laboratory accreditation discussions, and validation of the tool or the tool accreditation appears to be a concern. The distinction between validation and verification, ISO/IEC 17025:2017 describes them as follows:

> "**Verification**: provision of objective evidence that a given item fulfils specified requirements.
>
> **Validation**: verification, where the specified requirements are adequate for an intended use".

Regarding the tool and method requirements, Marshall and Paige (2018) articulate in their study that digital forensics method definition is an overlap in some degree between the requirements. In that study, there are three potential situations for overlap:

Scenario 1: Where the tool requirements are a subset of the method. This situation usually appears when specialist tools are being used, or a small tool is used to assist as part of the defined method.

Scenario 2: Where the method requirements are a subset of the tool. This scenario is rare, but it is possible when the method exactly follows the defined process by the producer of the tool, and that use is only a subset of the functionality of

the tool.

Scenario 3: Where there is an interaction in some degree between the tool requirements and method, and that is a common situation. In this case, the tool would interact with the method on all the technical requirements, but there will be other non-technical requirements, which are not fulfilled.

Marshall and Paige (2018) point out that during their research into the application of the mentioned mechanism in practice, that it is advised to allow the digital forensic tool producers to support their customers in the compliance of their laboratory for the ISO/IEC 17025 validation requirements. On the other hand, this support has to be performed, without the compromising of the sensitive information commercially, through the disclosure of the evidence tested. Unfortunately, that study failed to reach any valuable conclusion for the necessary information about the tool requirements because the inability of tool producers to cooperate in the study (small providers in this case) or unwillingly to disclose details on how they capture the customer requirements.

To address the interaction of ISO/IEC 17025 with the legislative Issues, Watson and Jones (2019) point out that the constant changes in the laws along with the rapid growth in the development of the technology, which results to a massive amount of opportunities for criminals to exploit it. For instance, within the United States law, the Daubert Standard is planned to be enforced for digital evidence, where it states that the digital evidence has to be a year or more behind in the way individuals and organisations tend to work. Another issue between the Daubert and ISO/IEC 17025 is the focus on the "error rates" that are associated with a tool or method. Scientific Working Group discussed this matter on Digital Evidence (2018) in its report regarding the digital forensic results by error mitigation analysis, where it highlights the fact that few numbers of errors can affect the outcome. The essential point in the error rate is that the main testing limitation, regardless of the amount of testing, has to prove the tool functions correctly. An unexpected result may result within a new scenario but it cannot occur without explanation (Sommer, 2018).

The consistency between the digital forensic tests is a primary factor in the success of each investigation stage, where the consistency between the processes generate consistency and repeatability to satisfy the court of law requirements. For instance, collecting digital evidence during the digital forensics acquisitive phase would effectively effect extracting the evidence and examine it in the laboratory

later. In other words, if data has been manipulated during the evidence acquisition or during transporting the evidence, this can affect the court case, even if the laboratory extract the data correctly and examine it correctly (Watson & Jones, 2019). The consistency between the digital forensic processes and activities through International Standards play a significant role in accepting the evidence by the jurisdiction in a defense or a prosecution, which is the whole purpose of establishing the case (Sommer, 2018; Veber & Klíma, 2014). Grobler (2012) report that the investigation cases which digital evidence was involved have a high rate of case dismissal due to the possibility of the risk of evidence collapsing under scrutiny. This is a direct contrast to the cases with non-digital evidence, and reflects on compliance to the ISO/IEC 17025.

2.5.2 Selected Issues and Problems.

The selected issues and problems found for the Standardisation requirements of digital forensic laboratories, relate to the use of general Standards not designed for digital forensic laboratories. The implementation requires compensation and tends to over burden organisations with activities that often cannot mitigate the scope of risk with digital evidence. In addition, the high costs due to the lack of consistency given its generic nature and required skill levels, result in multiple iterations of the implementation. The above analysis emphasises that ISO/IEC 17025 is overlapping with the ISO 9001 on designing the management system; thus, either of them is sufficient for covering all the aspects of the quality management system. The ISO/IEC 17025 is required to be mapped with the other ten digital forensics Standards to ensure the consistency over the whole timeline: pre-incident until the closure activity in the post-incident stage; especially with the incident management process, carried out by the ISO/IEC 27001:2017, which is considered the main driver to manage a whole case. Moreover, trimming the requirements in the ISO/IEC 17025 is mandatory since it contains non-applicable items for the digital forensic laboratory situation.

2.5.3 Problem Statement

The justice system prosecutes criminals and hears cases based on evidence. Digital evidence is volatile and requires expert assistance for the presentation. The handling

of digital evidence from collection to the Report presentation requires assurance that it has been factually preserved at each step in the chain of custody. Standardisation with networked use of International Standards can ensure the quality of the digital evidence processes and the trust others may put in the evidence. One of the critical areas is evidence examination within a laboratory. Here evidence has to be examined carefully to ensure the accuracy of the result. To Standardize a digital forensics laboratory requires a specific Standard. Researchers have demonstrated, and referred to in the literature, the absence of a specified digital forensics laboratory Standard, and yet after a decade the absence remains the same. Nevertheless, the ISO/IEC 17025, which is a general Standard for the competence of testing and calibration laboratories, can be adapted to accredit a specified digital forensics laboratory which requires expertise in the field to adjust the Standard to fit the requirements. Researchers articulated the requirement to establish a draft to build a new Standard in late 2000, and it is not yet complete. Thus, to fill this gap, this research has evaluated the relevant Standards, identified commonalities, and missing risk treatments. In addition, the literature is analysed to document how useful the digital forensic Standards are for improving practice, and what are the missing elements from the documents. Furthermore, the author articulates the adequacy of the guidance available for practice along with the analysis of the overlap between the International Standards to, directly and indirectly; implement the best practices for laboratories. Recommendations for this solution will be made for improvement and best practice guidance, with the development of drafting a new digital forensic Standard for digital forensic laboratories.

2.5.4 Selected Issues and Problems.

The potential solution to the problem focuses on four main dimensions, which are:

- The enhancement of the overlapping of the quality management system requirements between ISO/IEC 17025 and ISO 9001, which ensure the full coverage of all the aspects of the quality management system.

- Improving the consistency between the overlapped Standards during the digital forensic lifecycle pre-incidence and post-incident; especially the interaction of the digital forensic laboratory activities with the incident management.
- Eliminating the unnecessary elements within the ISO/IEC 17025, which are not applicable to the digital forensic laboratory.
- Analyse the missing elements within the ISO/IEC 17025, which are necessary to fill the gap and articulate the missing points.

2.6 CONCLUSION

The absence of one unified digital forensic Standard opens the discussion for the use of a set of interoperable Standards, where each Standard either plays a role in covering one or more of the digital forensics processes and activities or completes the missing gap in one of the Standards. The ISO/IEC 27000 family documents play a significant role in the digital forensic investigation. Ten Standards interact with the digital forensic life cycle during the following phases: Readiness, Initialization, Acquisitive, and Investigative processes. In addition to that, there are several related Standards from other ISO groups, which contribute to a forensic laboratory requirement. The ISO /IEC 17025 is an applicable normative Standard specifying the general requirements for the competence of the laboratory's operation, which may be used to accredit a digital forensic laboratory. The ISO/IEC also has a competency-based ISO 9001 as the management Standard to build the QMS. It also fills the gap in the management system section in the ISO/IEC 17025. In Chapter 3 a methodology is to be specified to address the issues and problems identified in this chapter, and a pathway forward defined for writing a draft Standard to fill the identified gaps in the current literature.

Chapter 3: Research Methodology

3.0 INTRODUCTION

In Chapter 2 the problems and issues with current standardisation for digital forensics laboratories was summarised from the literature. In this chapter, an explanation of the methodology to solve the problems, is identified. In addition, it is explained in this chapter how the researcher conducts the analysis for the literature review, and the research gap analysis. The PRISMA method has been used to conduct the literature search for this research. Since this thesis is theoretical research with literary analysis, and a guideline and Standard construction for the digital forensic laboratory; design science (DS) had been used as a research methodology to produce an artefact and the quality improvement. The chapter is structured to locate the research objective and questions, and then to formalize the methods.

3.1 RESEARCH OBJECTIVE

This research aims to fill a gap in literature where there is currently not International Standardisation for digital forensic laboratories. One of the essential objectives of the research is to provide a best practice guideline for the Standardisation of digital forensic laboratories. By the contextual analysis of the identified problems, this thesis aims to treat the inherent risk from the absence of a digital forensic laboratory Standard. The artefact will positively affect the acceptance of digital evidence to be used in legal proceedings. Furthermore, recommendations are made to encourage the field experts to eradicate the identified problems that surround the accreditation of the digital forensic laboratories by the establishment of an International Standard specified for this type of laboratory.

3.2 RESEARCH QUESTIONS

Several questions have been chosen for this research, based on reaching the goal of the study. The stated questions were designed to be focused on a solution artefact for the problem statement. The research questions are as follows:

- What are the Standardization requirements for a digital forensic laboratory?
- How useful are these Standards for improving practice?
- What elements are missing from the documents?
- What is the adequacy of the guidance available for practice?

3.3 RESEARCH METHODS

In this section, the research methods that are used in this thesis will be explained, starting with the utilization of a well-known method to conduct the systematic and structured literature review presented in Chapter 2. The literature search subsection articulates the overall structure of how the literature is being searched, selected, and filtered based on pre-defined criteria. Later, the subsection on DS research methodology presents and explains the main methodology used in this research. The subsection includes the explanation of the methodology lifecycle supported by a review of six previous studies with the process elements of the methodology.

3.3.1 Literature Search.

In this thesis, a systematic and structured literature review has been used to analyse the literature, which resulted in a gap analysis. Investigating the gap presented the inconsistency in the International Standardisations that are applicable for digital forensic laboratories. The systematic literature review was conducted using the PRISMA guideline (http://www.prisma-statement.org). This guidance for the systematic review was started under the name of QUOROM Statement (Quality of Reporting of Meta-analyses). The documentation in 2009 to address methodological, practical, and conceptual advances and renamed to PRISMA (Moher, Liberati, Tetzlaff, & Altman, 2009; Tao et al., 2011). PRISMA can be applied in a literature search through four stages: identification, screening, eligibility, and the included. The identification stage presents the records that have

been identified through database searching including the name of the database(s) and dates of the search period. Also, all the duplicates records must be removed in the transition to the next stage. In the screening stage, the number of records that are screened is presented along with the number of excluded references. After that, a full-text reading has to be applied, and assessed for eligibility and excludes the ineligible citations by specifying the reasons. This stage is called the eligibility stage. Finally, the last phase includes the citations that are to be involved in the qualitative synthesis for the research literature (Gómez-Ochoa, Ortega-Chasi, Alvarado-Cando, Cobos-Cali, & Artega-Sarmiento, 2020; Liberati et al., 2009; Moher et al., 2009). Figure 3.1 presents the information flow of the PRISMA phases.

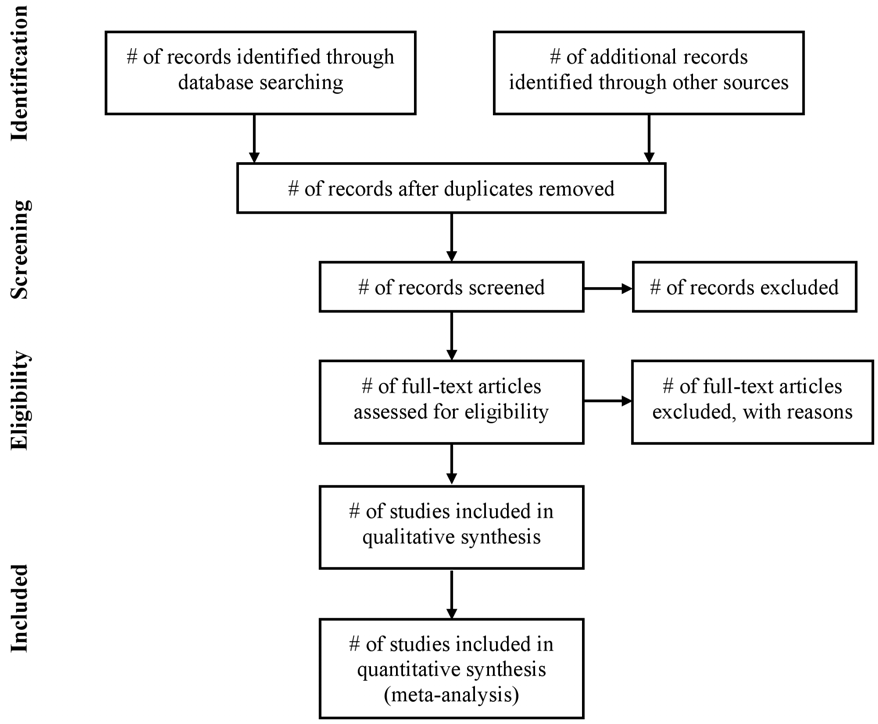


Figure 3.1: Flow of information in the PRISMA phases. Reprinted from Preferred Reporting Items for Systematic Reviews and Meta-Analyses: The PRISMA Statement (p.3), by Moher, D., Liberati, A., Tetzlaff, J., & Altman, D. G., 2009, British Medical Associati

In the literature search, the author used search terms to find previous studies, which contribute to answering the research questions. These search chains were conducted in English according to the search terms. In addition, AND and OR, and quotation were used in the search, to limit the research results in to a manageable quantity. The application of the search terms to the metadata was specified to cover the article title, abstract, and keywords. The search terms were redefined by the researcher

each time new information was found on one of the citations, to further analyse the literature in-depth. In Table 3.1, the main keywords used in the search are listed.

Table 3.1: The searching keywords.

Searching keywords
"Digital" AND "Forensic" AND "Accreditation" AND "Laboratories" OR "Laboratory"
"digital" AND "forensic" AND " Standard"
"digital" AND "forensic" AND "17025"
"digital" AND "forensic" AND "9001"
"digital" AND "forensic" AND "27035"
"digital" AND "forensic" AND "27037"
"digital" AND "forensic" AND "27038"
"digital" AND "forensic" AND "27040"
"digital" AND "forensic" AND "27041"
"digital" AND "forensic" AND "27043"
"digital" AND "ISO" AND "27050"
"digital" AND "ISO" AND "30121"

The search was conducted between July 16, 2019, to September 2, 2019. Three main databases were used during the search: British Standards Institution (https://bsol.bsigroup.com), IEEE Xplore Digital Library (https://ieeexplore.ieee.org), and Scopus (http://www.scopus.com).

The search was conducted using the following search criteria:

- **Year of publication**: Since the QMS Standard was published back in 1999, which is a primary part of the ISO 17025 Standard, that year of publication was set to limit publications released before 2000.
- **Language**: References were written in English only.
- **Publication stage**: Only final.

After the search, the author scanned the result to ensure the result met the defined inclusion and exclusion criteria. The following criteria are:

- **Inclusion Criteria:** Only studies dealing with the following areas: Information security incident management, security techniques in managing digital evidence, digital redaction, storage security, incident investigative method, Analysis and Interpretation of digital evidence, security information and event management, electronic discovery, and business forensic governance.
- **Exclusion criteria:** Studies which are not relevant to the defined area in the inclusion criteria.

The author has used PRISMA as a strategy to extract data, and the application of the systematic review steps of this thesis are summarised in Figure 3.2.

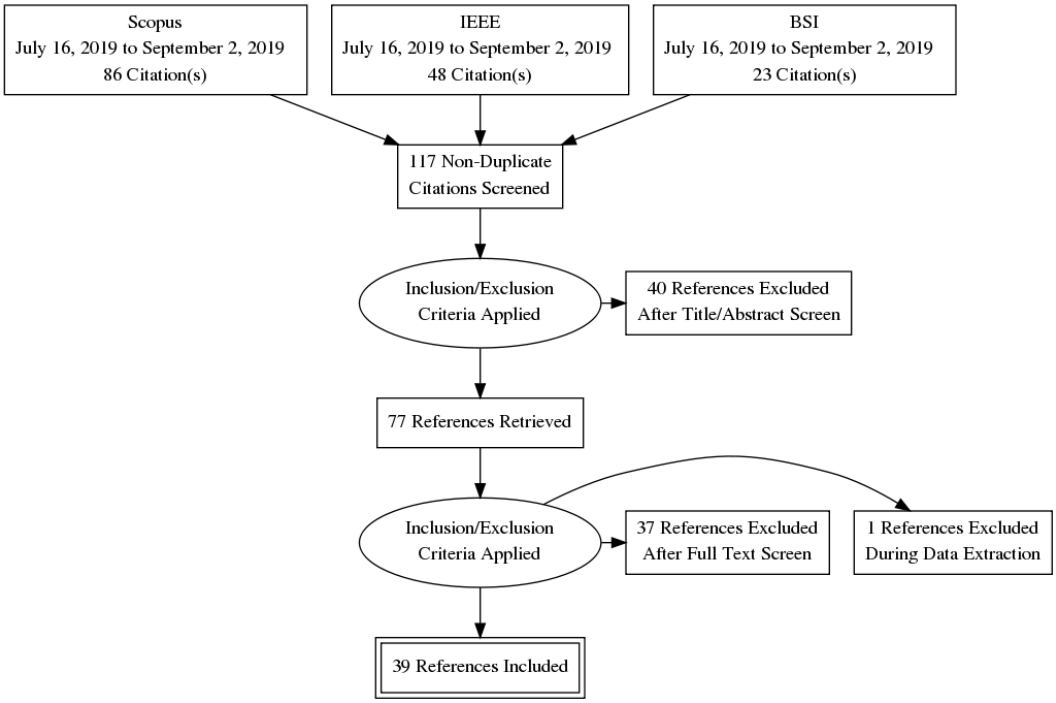


Figure 3.2: The flow of information on the application of PRISMA in this research.

3.3.2 Design Science Research Methodology.

Design Science (DS) research methodology has been used in this research to design a proposed solution to the identified problems. The selection contributed to the thesis research by the use of a commonly used methodology with its legitimation and recognition in the computer sciences researches domain. DS can be defined as designing and investigating an artefact in a particular context, where the designed

artefact is to be studied to improve the context by interacting with the problem context (Peffers, Tuunanen, Rothenberger, & Chatterjee, 2007; Wieringa, 2014). Wieringa (2014) illustrates that the artefact concept has to be taken broadly, where even conceptual structures can be considered as a valuable artefact for a particular purpose. Wieringa (2014) explains that the appearance of values, budgets, fears, desires, norms, and goals can be provided to the design researcher only as a part of the problem context, and these elements have to be considered during the investigation and design of the artefact, but it cannot be designed as an artefact. Furthermore, the artefact solves the problems by the interaction with the problem context, not the artefact itself alone; therefore, the design researcher should study both the context and the artefact together rather than study each one of them separately.

According to Peffers et al. (2007), the DS lifecycle consists six elements: problem identification and research motivation, objectives of the solution, design and development of the artefact, demonstration, evaluation, and communication. The DS process model is in Figure 3.3. In Table 3.2, the author compared these process elements to several other researchers' ideas in the IS and other fields, which resulted in the similarity of the common elements. Thus, the author used these processes in this thesis due to substantial agreement on the processes order.

Table 3.2: The processes and elements of the DS from IS and other disciplines and synthesis on these elements in IS.

Common criteria elements	Hevner and Chatterjee (2010)	Walls, Widmeyer, and El Sawy (1992)	Nunamaker Jr, Chen, and Purdin (1990)	Eekels and Roozenburg (1991)	Takeda, Veerkamp, and Yoshikawa (1990)
Problem identification and motivation.	Important and relevant problems that can be solved by a technology-based solution.	Meta-requirements	Construction of conceptual frameworks.	Problem analysis.	Enumeration of problems
Solution objectives.		Meta-design and design methods.	Building and observing the theory strategies.	Requirements	Suggestion and development

Artefact design and development	Design a viable artefact to the identified form.		Constructing the architecture of the system after designing the concept, prototyping, product development, and technology transfer of the Systems development.	Synthesis and tentative design proposals.	
Demonstration	The produced solution must have verifiable contributions, which demonstrate the effectiveness of the solution. Also, research must be rigor.		laboratory experimentation including experimental simulations.	Simulation and conditional prediction.	
Evaluation		Testable design product and process hypotheses	Validation of the underlying theories.	Evaluation, the value of the design proposals, detection, and defining the design.	Evaluation to confirm the solution.
Communication	Communication of research.				

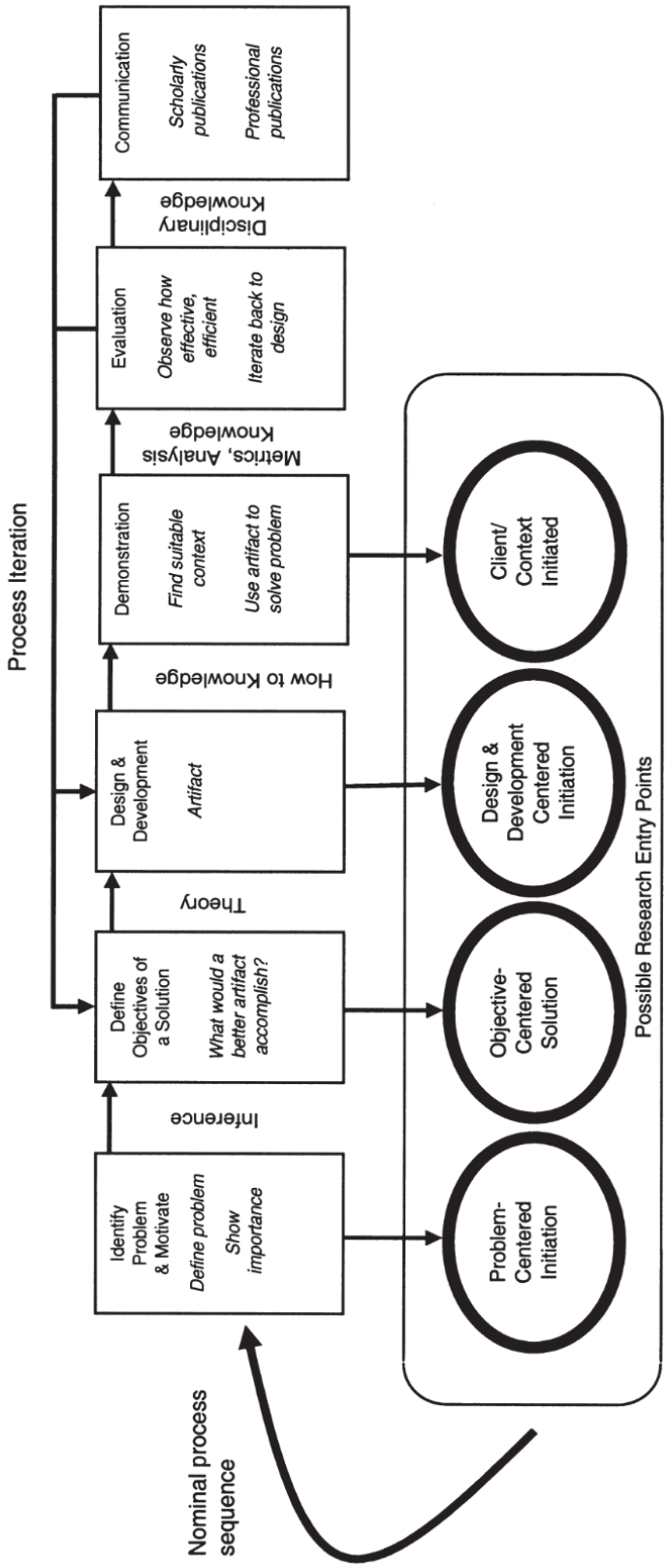


Figure 3.3: The DS Process Model. Reprinted from "A design science research methodology for information systems research," by Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S, 2007, Journal of management information systems, p. 54.

The DS consists of two parts, which are design and investigation. Besides that, there are what is called research problems, which divided, into two main parts: design problems and knowledge questions. Wieringa (2014) points out that there is one possible sequence to start with the design problems, which lead to the knowledge questions of the artefact. The activity of answering the knowledge questions returns knowledge to the event of solving the problem; conversely, answering the knowledge questions can lead to the existence of a new design problem. Design problems can be defined as the elements to design and redesign the targeted artefact to achieve the planned goal of the research (Wieringa, 2014). The knowledge questions are refined from the project knowledge goals, where these questions are answered without requesting an improvement (Wieringa, 2014). Therefore, problems can lead to the creation of new issues, which is the provision that a DS is not restricted only to one type of a problem.

As identified in Figure 3.3, the application of the DS in this thesis started by defining the problems and analysing the gap in the Standardisation requirements for the digital forensic laboratory. These issues and problems have been identified in the literature chapter, and recapped in the following *Design problem* and *Knowledge questions* in Table 3.3.

Table 3.3: The thesis' DS research problems.

Design problem	Knowledge questions
Ditch the not compliance elements of the digital forensic laboratory from the ISO/IEC 17025 Standard.	Is the rest of the elements being mandatory?
Map the overlapped processes from other ISO Standards.	Are all the overlapped processes comply with the digital forensic laboratory requirements?
Design the guideline document to compliance the Standardisation requirements to the digital forensic laboratory.	Are there any missing pieces? Is this verified in the field with experts?

Design a Standard draft to Standardize digital forensic laboratories.	Is this draft usable and useful for all digital forensic laboratories? Is it accurate enough?

After the review and analysis of the previous studies, problems have been identified, and design problems have been produced along with the knowledge questions; and, the Engineering Cycle (EC) has been applied to solve the issues. According to Wieringa (2014), EC can be defined as rational problem-solving iterations, where the following lifecycle is performed:

- **Problem investigation:** Improvement opportunities? Importance of improvement?
- **Treatment design:** Designing an artefact or more than one to solve that problem(s).
- **Treatment validation:** Would the designed artefact(s) treat the identified problem(s)?
- **Treatment implementation:** Treating the problem(s) with the artefact to observe the effectiveness of the treatment**.**
- **Implementation evaluation:** Evaluate how successful the treatment was!? In this point, the artefact might require a redesign if the review is negative.

Within these stages, problems have been identified previously. It is the importance of solving the issues around the absence of a Standard dedicated for the digital forensic laboratories. The developed draft Standard is the result of the treatment design. Besides that, the treatment validation has proceeded with several digital forensic experts, in Chapter 6, to validate the effectiveness of the proposed solution to the identified issues. The full implementation shall be carried after the expert feedback, which is outside of the research scope; and the scope of this research is

limited to the first three phases of EC as per the methodology journey that is presented in Figure 3.3.

In the validation stage, questions had to be asked to ensure the effectiveness of the proposed solution. These questions are required to be designed in alignment with the primary goal and objective of the research, but it has to be differentiated. The questions were designed based on three main evaluation streams: goal, environment, and activity (dynamic, the operations and functionality of the artefact). The goal stream of the evaluation questions evaluates the efficacy and validity of the produced artefact, where the activity stream focuses on completeness. The environment stream focuses on the consistency with the organization and people, where people are evaluated on the utility, understandability, and easiness dimensions. The evaluation criteria and questions can be seen in Table 3.4. In this thesis, the primary goal is to Standardize the best practices of digital forensic laboratories primarily in order for the examined evidence to be accepted in court. The treatment validation has to cover how broadly this artefact treated the gap through the Standardisation requirements of the digital forensic laboratories. The last two stages of the EC are considered as future actions required to be carried through a field implementation in a real environment.

Table 3.4: The evaluation criteria and questions.

Measurement and evaluation	Evaluation criteria	Sub-criteria	Questions
Goal	Efficacy		Q: How effective do you think the proposed Standard would be in covering the Digital forensic laboratories requirement?
	Validity		Q1: Are the defined clauses and sub-clauses in the draft Standard are relevant to what you observe in your area of expertise? Q2: Are the provided metrics adequate and helpful to determine relevant mitigation measures? Q3: Is the provided strategies' payoff guidance realistic and

			adequate?
Environment	Consistency with people	Utility	Q1: Do you think the draft Standard is effective and efficient in guaranteeing the digital evidence integrity? Q2: Do you think the draft Standard is effective and efficient in Standardizing the best practices of the DF? Q3: How effective do you think the digital forensic laboratories will be if more DF experts start using produced guideline?
		Understand- ability	Q.1 How easy it was to evaluate the draft Standard, and was there any difficulty in evaluating it? Q2. How long did it take you to go through each component from start to finish? Was that reasonable? Q3. Were the provided instructions helpful/clear?
		Ease of use	Q: Usability and ease of implementation?
	Consistency with organization	Utility	Q: Does the designed Standard guideline have the potential to be widely adopted?
Activity (Dynamic, the operations and functionality of the artefact)	Completeness		Q1. What are the areas that can be improved? Please do not hesitate to list as many as you want. Q2: Modification needed? Q3. Strengths and weaknesses of the draft Standard? Q4. How complete do you think the Standard guideline is?

3.3.3 Conclusion.

The research objectives have been identified in this chapter along with the research questions. In this thesis, PRISMA has been used for systematic and structured literature review, which have been used and analysed to identify the problems. Within the PRISMA lifecycle, more than a hundred citations have been screened on a high level, which resulted in 77 references after the inclusion and exclusion criteria have been applied. Moreover, a full-text screen details, which results in the included references within the research literature, are to be cited. DS has been used as a methodology for this research, where it consists of six stages. The first stage starts by identifying the problems and the motivation to solve these issues. Then the solution objectives have to be pointed out. Moreover, the artefact is designed and developed based on these stages in the third stage. After that, identifying a suitable context to use the artefact and observe the effectiveness and efficiency of the artefact comes as two linked stages: demonstration and evaluation. The result of these two stages determines whether the research should be driven in a direct to re-design the artefact or to accept the artefact as a solution to the problem in a specified context. If the solution is approved, this will direct the research to the final stage, which is the communication (publication).

Chapter 4: The Draft Standard

4.0 INTRODUCTION

This chapter takes into consideration the specific requirements of the digital evidence environment and the importance of the digital forensic laboratory to evidential assurance. This chapter contains requirements for digital forensic laboratories to enable them to demonstrate they operate competently, consistently, and in a trustworthy fashion that others may have confidence in the veracity of the digital evidence. This chapter requires the digital forensic laboratory to plan and implement actions to assure potential points of failure are addressed, and management measures are continuously improved for optimal effectiveness. The volatility of digital evidence requires special attention for preventative and corrective actions that assure storage, processing and transportation integrity. Management is responsible for conformance and the trust others may have in the quality of the digital forensic services.

The use of the proposal in this chapter will facilitate consistent digital forensic laboratory services that conform to the customer expectations for evidential purposes. It will promote confidence that the services are fit for purpose and the ability for the transfer of digital evidence from one locality and user, to another.

In this chapter, the following verbal forms are used:

— “shall” indicates a requirement;

— “should” indicates a recommendation;

— “may” indicates a permission;

— “can” indicates a possibility or a capability.

Further details can be found in the ISO/IEC Directives, Part 2. The presentation of this Chapter is structured to conform with a ISO/IEC SC27 documentation for a draft standard so that in the future it may be taken by others to start the negotiation processes through a NWIP submission.

4.1 SCOPE

This draft Standard specifies requirements for competence and quality in digital forensic laboratories. This draft Standard can be used by digital forensic

laboratories in developing their QMS and assessing their own competence.

4.2 NORMATIVE REFERENCES

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 27038:2014, Information technology. Security techniques. Specification for digital redaction

ISO/IEC 27041:2015, Information technology. Security techniques. Guidance on assuring suitability and adequacy of incident investigative method

ISO/IEC 27042:2015, Information technology. Security techniques. Guidelines for the analysis and interpretation of digital evidence

ISO/IEC 27043:2015, Information technology. Security techniques. Incident investigation principles and processes

ISO/IEC 27050-3:2017, Information technology. Security techniques. Electronic discovery. Code of practice for electronic discovery.

EN IEC ISO 22301:2019, Security and resilience. Business continuity management systems. Requirements

EN ISO/IEC 27001:2017, Information technology. Security techniques. Information security management systems. Requirements

ISO/IEC 27002:2013, Information technology. Security techniques. Code of practice for information security controls

ISO/IEC 17025:2017, General requirements for the competence of testing and calibration laboratories

ISO/IEC 27037:2016, Information technology. Security techniques. Guidelines for identification, collection, acquisition and preservation of digital evidence

ISO/IEC 24775-1:2014, Information technology – Storage management – Part 1: Overview

ISO/IEC 24775-8:2014, Information technology – Storage management – Part 8: Media libraries

ISO/IEC 27040:2015, Information technology. Security techniques. Storage security

4.3 TERMS AND DEFINITIONS

For the purposes of this document, the terms and definitions given in ISO/IEC 17025, ISO/IEC 17025, ISO/IEC 27037, ISO/IEC 27038, ISO/IEC 27041, ISO/IEC 27042, ISO/IEC 27043, BS ISO/IEC 27050-3, and ISO 9000:2015 apply.
ISO and IEC maintain terminological databases for use in Standardization at the following addresses:
• ISO Online browsing platform: available at http://www.iso.org/obp
• IEC Electropedia: available at http://www.electropedia.org/.

4.4 MANAGEMENT REQUIREMENT

To cover the management requirements, this section mainly covers, through the following subsections, the organization, management responsibility, and the quality management system. The "organization" subsection covers the primary requirements to have a legitimate entity, scoped properly, function on an ethical bases, and have a director; which the highest authority in the laboratory. In addition, the "Management responsibility" subsection covers what the management of the laboratory shall ensure to have available. This includes the commitment of the management, the requirements of the user, quality policy, the objective and planning of the quality, responsibilities of who shall carry out the defined tasks, the communication of the laboratory, and the laboratory quality manager. Lastly, the "quality management system" subsection presents the requirements of establishing a comprehensive quality system to articulate how the laboratory can meet the requirements in the draft Standard.

4.4.1 Organisation and Management Responsibility

The following subsections present the organizational requirements and the responsibility of the laboratory management that shall be taken into consideration.

4.4.1.1 Organisation

The following subsections cover the organizational requirements including:
— What shall a digital forensic laboratory meet on an enterprise-level;

— The legal perspective that a digital forensic laboratory shall take into consideration;
— The requirements of the ethical conduct of the laboratory;
— The requirements of the authorization and delegation of a laboratory director.

4.4.1.1.1 General requirements

The digital forensic laboratory shall ensure meeting the requirements of this draft Standard during the carrying out of its activities at its permanent and mobile facilities, or in its any associated facilities.

4.4.1.1.2 Scoped and legalised entity

The digital forensic laboratory management shall ensure to have arrangements in order to ensure the following:
1) That there is no involvement of any type by any party, which may diminish the confidence of the integrity of the digital forensic laboratory in its operation, impartiality, judgement, or competence;
2) The digital forensic laboratory employees shall be free from any excessive commercial, or/and financial influence. Also, they should not any constrain or pressures that may influence the quality of the work, direct or indirect;
3) In the case of the potential of the existence of any type of conflicts of interests, these conflicts shall be declared in an open and appropriate manner;
4) The assurance of handling any type of digital evidence in accordance with legal requirements, including the governance and control of the handling procedures;
5) Confidentiality of information or any relevant activities to the work is maintained that may or may not affect the integrity of the digital forensic laboratory.

4.4.1.1.3 Laboratory director

The person who manages the laboratory (hereinafter referred to as ‘the director’) shall be authorized to perform the delegated responsibility for the provided services by the digital forensic laboratory. The director shall be responsible for all the organizational, advisory, professional, administrative, educational, and scientific matters provided by the digital forensic laboratory;

The director shall be responsible for the Responsibility Assignment Matrix (RAM), known as the RACI matrix, of the digital forensic laboratory. (see 4.4.1.2.5).
The director can delegate and revoke responsibilities or/and duties only to the qualified personnel, and the RAM shall be updated if this activity impacts the maintenance of the accountability of the director of the overall operation and/or administration of the digital forensic laboratory. The director responsibilities shall be documented and maintained as part of the RAM.

The director, or who is delegated to perform duty(s), shall:

a) Perform an effective leadership of the digital forensic laboratory and provide services in accordance with the organization strategic drivers;

b) Relate and function effectively when required with the digital forensic laboratory' internal and external community including regulatory agencies and jurisdiction.

c) Ensure there is an appropriate number of resources to meet the requirements in preforming the digital forensic laboratory services to ensure fulfilling the customer requirements.

d) Ensure that the digital forensic laboratory' quality policy is implemented fully;

e) Ensure the competency of the digital forensic laboratory' environment to the common best practices;

f) Function effectively as a part of the digital forensic laboratory community;

g) Ensure that the digital forensic laboratory' suppliers are selected and periodically reviewed in accordance with the need of the laboratory.

h) Ensure the laboratory provides personal professional development programmes for staff, with the opportunities for staff to participate in related professional organization activities in alignment with the defined tasks in the laboratory RAM.

i) Define, plan and monitor related Standards that influence the digital forensic laboratory services, or delegate this responsibility to accredited personnel with full accountability on the director.

4.4.1.2 Management responsibility

The following subsections present the responsibilities that shall be taken into consideration by the digital forensic laboratory management. It has the following subsections: the commitment of the management, the requirements of the user, quality policy, the objective and planning of the quality, responsibilities of who shall

carry out the defined tasks, the communication of the digital forensic laboratory, and the digital forensic laboratory quality manager.

4.4.1.2.1 The commitment of the laboratory management

Evidence of the management committee of the digital forensic laboratory shall be provided in the case of developing and implementing the quality management of the laboratory, and maintaining it continually through:

a) communicating with the digital forensic laboratory staff continually the importance of maintaining the regulatory and accreditation requirements along with the users' needs (see 4.4.1.2.2);

b) the establishment of the quality policy of the digital forensic laboratory (see 4.4.1.2.3);

c) ensure the quality objectives and the strategic plan of the digital forensic laboratory is established (see 4.4.1.2.4);

d) define the accountabilities and responsibilities of the personnel and link it to the digital forensic laboratory tasks list (see 4.4.1.2.5);

e) ensure to conduct periodic management reviews (see 4.4.2.15);

f) ensure the competence of the laboratory' personnel to perform the defined tasks and activities in the digital forensic laboratory RAM;

g) the establishment of communication processes in accordance with the defined communication roles in the RAM (see 4.4.1.2.6);

h) appointing and delegating a digital forensic laboratory' quality manager (see 4.4.1.2.7);

i) ensure the availability of adequate personnel resources (see 4.5.1) in order to guarantee the enablement of the digital forensic laboratory to perform the agreed services (see 4.4.2.4).

4.4.1.2.2 The user requirements

The management of the digital forensic laboratory shall ensure the provided services meet all the customer requirements that are established in the customer agreement (see 4.4.2.4.1).

4.4.1.2.3 Quality policy

The intent of the Quality Management System (QMS) shall be defined by the digital forensic laboratory management, and the responsibility to ensure the quality policy, as follows:

a) is aligned with the digital forensic laboratory organizational drivers;

b) commitment to the professional practice of the digital forensic laboratory activities including the surety of the fit of the activities to the intended use along with the continuous improvement of the policy to the provided services;

c) provides a framework for the establishment of the objectives of the quality policy, and ensure it is being reviewed regularly;

d) ensure the understanding of the policy across the organization;

e) provide evidence for the regular review of the quality policy to ensure its suitability.

4.4.1.2.4 The planning and objectives of the laboratory quality

The quality objectives shall be established by the management of the digital forensic laboratory; the objectives of the laboratory shall be measurable and in alignment with the quality policy.

The management of the digital forensic laboratory shall ensure the fulfilment of the Quality Management System (QMS) planning to and the requirements in general and the defined quality objectives. (see 4.4.2).

The management of the digital forensic laboratory shall ensure the maintenance of the QMS integrity during the establishment and when a change is planned, and executed.

4.4.1.2.5 Responsibility, accountability and interrelationships

The management of the digital forensic laboratory shall ensure the definition, documentation, and communication of responsibilities, accountability and interrelationships. This shall include the definition of the digital forensic laboratory tasks and the interrelation to the accountability, responsibility, consultant, and information to personnel; this is defined as the digital forensic laboratory RAM.

4.4.1.2.6 Communication

The management of the digital forensic laboratory shall have an effective communication method with the digital forensic laboratory staff. The communication records shall be stored in a defined sequel for future purposes. The management of the digital forensic laboratory shall ensure the establishment of effective internal communication via the digital forensic laboratory RAM; also, the management shall ensure the establishment of communication processes between the digital forensic laboratory and its stakeholders in the manner of the laboratory activities and its QMS.

4.4.1.2.7 The digital forensic laboratory quality manager

The management of the digital forensic laboratory shall appoint a quality manager, who handles the following responsibilities:

a) Carry out the establishment and maintenance of the digital forensic laboratory QMS and ensures the competence of the system during the execution and overall;

b) Directly reporting to the director regarding the objectives, resources, and the performance of the digital forensic laboratory QMS including its continuous improvement.

c) Ensure the awareness of the QMS across the organization including the necessity of fulfilling the customer requirements.

4.4.2 Quality Management System

The following subsections present the requirements for the establishment and maintenance of a QMS for digital forensic laboratories. These include general requirements, documentation requirements, document control, the digital forensic laboratory service agreements, examination by referral digital forensic laboratories, external services and supplies, the digital forensic laboratory advisory services, handling complaints, managing nonconformities, corrective and preventive actions, continuous improvement, control of the digital forensic laboratory records, evaluation and audits, management review, and ensuring the continuity of the business.

4.4.2.1 General requirements

A QMS for the digital forensic laboratory shall be established, implemented, documented, and maintained continuously.

The quality policy and its objectives shall be fulfilled by a comprehensive integration of the QMS processes in order to meet user needs.

The digital forensic laboratory shall:

a) Ensure the determination of the required processes of the QMS, along with its application across the digital forensic laboratory;

b) Ensure these processes are determined and well integrated and consistent;

c) Ensure the existence of criteria and methods to ensure the effectiveness of these processes;

d) Ensure the availability of the necessary information and resources, which are required to support operating and monitoring these processes;

e) Ensure the capability to monitor these processes and guarantee a continuous evaluation.

f) Implement the necessary actions to ensure the achievement of the planned objectives and goals, along with a guarantee for the existence of the continuous improvement of these processes.

4.4.2.2 Documentation requirements

The following subsections cover the requirements of the documentation of the QMS, and the requirement to the establishment and maintenance of the laboratory Quality Manual (QM).

4.4.2.2.1 General requirements

The digital forensic laboratory shall assure the existence of a QMS documentation; including:

a) A manual of the digital forensic laboratory quality (see 4.4.2.2.2);

b) Quality policy statements (see 4.4.1.2.3) and quality objectives (see 4.4.1.2.4);

c) The proper records and documents (see 4.4.2.13), which ensure that the processes planning, implementation, operation and control are effective;

d) Copies of the regulations, and related documents and Standards to the QMS.

4.4.2.2.2 The laboratory quality manual

The digital forensic laboratory shall ensure the establishment and maintenance of a Quality Manual (QM); the QM shall include:

a) The laboratory QMS scope description;

b) A copy of the laboratory quality policy referenced by the version (see 4.4.1.2.3);

c) Structure of the organizational hierarchy, including the digital forensic laboratory hierarchy to the parent organization;

d) A copy of the digital forensic laboratory RAM, including the responsibilities of the director and the appointed quality manager;

e) The established and implemented laboratory policies for the QMS and the activities of the supportive technical and managerial;

f) The QMS documents structure and relationship.

The digital forensic laboratory shall ensure and document the recruitment of the QM, along with the guarantee of the full access of the staff to the QM.

4.4.2.3 The laboratory document control

The digital forensic laboratory shall ensure the control of the related documents that are required by the digital forensic laboratory QMS and shall ensure the misuse prevention of obsolete documents. This is all information from a point in time to be contained in the records, which point to the results achieved or provide evidence that a particular activity has been performed in accordance to the requirements of the control of records (see 4.4.2.13). The referred documents are the ones, which have a wide scope and based on any changes that are reflected by an update on the document version. These changes include, but are not limited to, any addition, modification, and/or removal of any item of the document.

The existence of a documented procedure has to be ensured by the digital forensic laboratory to meet the following:

a) All the documents have to identify:

— The digital forensic laboratory header including the logo and the legal name and license which the digital forensic laboratory is operating based on;

— a title;

— the unique identifier of the document on each page and a unique identifier of

each page next to it;
— the current edition number and edition date;
— page number to the total number of the document pages;
— the authorized issuer.
b) The latest authorized editions and its distribution have to be identified in any type of list.
c) The applicable documents, which are available for use, have to be the latest authorized editions
d) If the document control system of the digital forensic laboratory allows the documents amendment by hand while waiting for the digital document to be re-issued, then, in such an amendment, the procedures and authorities have to be written clearly, dated, and signed. This amendment is valid until this document is re-issued and approved or for a defined period of time.
e) A sequel of documents changes are identified and recorded.
f) The documents shall remain legible.
g) Ensure the documents are fit for purpose by a periodic review.
h) One or more copy of the obsolete controlled documents has to be retained for a defined period of time.
i) Any controlled document, which is obsolete, shall be stamped with the date and signed as an obsolete document.
j) The necessary of reviewing and approving all digital and/or paper-based documents, which are released as part of the QMS by the authorized personnel before the issue. An authorization has to be approved as part of the digital forensic laboratory RAM.

4.4.2.4 Service agreements

The following subsections cover the establishment of the service agreement with the customers and ensure the update of any affected party if any amendments to the agreement are made.

4.4.2.4.1 The establishment of the service agreements

The establishment of the service agreement shall be carried out by the digital

forensic laboratory through documented procedures, where any accepted request to the digital forensic laboratory is considered as an agreement. The agreed services agreement shall take into consideration, at least, the service priority, evidence examination, and the result report along with the final statement. In order to ensure the accuracy of the examination result, all needed information shall be specified in the agreement. If the result of the examination would be presented in any legal jurisdiction, the digital forensic laboratory shall ensure the existence of a process to consult an internal or external legal division. If the legal division is an external division, the digital forensic laboratory shall ensure the existence of a prior contract including, but not limited to, a non-disclosure agreement.

During the establishment of a services agreement, a set of conditions, but not limited to, shall be met:

a) The agreement party requirements shall be documented after it is been identified and understood.

b) The availability of the resource(s) in order for the requirements to be met shall be assured prior by the digital forensic laboratory.

c) The digital forensic laboratory shall ensure that the personnel have the necessary skills and expertise to perform the examinations.

d) The selected procedures for the digital forensic laboratory examinations shall meet the requirements of the customers.

e) The digital forensic laboratory shall ensure that the customers are informed formally in the case of any deviations that may or may not affect the examination results.

4.4.3.4.2 Review of the service agreement

The digital forensic laboratory shall review its service agreements and update any affected party if any amendments are made. The record of the agreement shall contain all versions.

4.4.2.5 Examination by referral digital forensic laboratories

The following subsections cover the selection and evaluation of the referral digital forensic laboratories and/or consultants, and the requirements to provide the results of the examination that are performed by a referral laboratory.

4.4.2.5.1 Select and evaluate referral digital forensic laboratories and/or consultants

The digital forensic laboratory shall ensure the existence of a documented procedure on selecting and evaluating referral consultants and/or laboratories, which support the laboratory services by providing their opinions.

The following conditions shall be met in this procedure.

a) Monitoring the examination of the referral laboratories until the request is completed shall be performed by the digital forensic laboratory, which has an agreement with the customer.

b) The agreements with the referral digital forensic laboratories and/or consultants shall be evaluated and reviewed periodically.

c) These periodic reviews are recorded and documented.

d) All the referral digital forensic laboratories and/or consultants have to be documented in a register electronically.

e) All the referred requests and results are documented and recorded, and stored for a defined period.

4.4.2.5.2 The provision of laboratory examination results

The delivery of the result of the examined evidence shall be provided by the referring digital forensic laboratory. The referring digital forensic laboratory shall be responsible for the final report to the customer, including but not limited to the examinations that have been performed by the referring or/and referral laboratory. The examinations that been performed by the referring or/and referral laboratory shall be the same as the agreed examinations stated in the service agreement. The manner of reporting an examination is to be standardized, and to use the most adequate method in reporting. The results of the examinations may be transferred electronically from the referral laboratory to the customer and the communication shall be documented.

4.4.2.6 The external supplies and services

The digital forensic laboratory shall ensure the existence of documented processes in the selection and purchasing of any external elements. This includes but is not

limited to: equipment, expertise, and any laboratory elements that may or may not involve in the examination quality. The digital forensic laboratory shall ensure it has an up to date approach to the select and approve of any suppliers that have direct or indirect business with the digital forensic laboratory. This approach shall be based on the technical ability of the suppliers to meet the laboratory requirements. The digital forensic laboratory shall have a register list of all the, approved or non-approved, external suppliers including the responses for rejection. The list shall be updated regularly based on a pre-defined time (e.g. weekly or monthly).

The digital forensic laboratory shall ensure the following conditions are met in its Request for Proposal (RFP) to any external supplier:

a) The RFP is approved, and the approval dated by the director, or who is delegated on behalf;

b) A pre-defined time to accept the proposals from the supplier;

c) A detailed description of the required product or service.

The digital forensic laboratory shall ensure monitoring the digital forensic laboratory supplier performance periodically based on a pre-defined criterion.

4.4.2.7 Advisory services

The digital forensic laboratory shall ensure the establishment of arrangements in its communication with its users, or potential users, by the following:

a) Promoting the digital forensic laboratory services;

b) Advising on the need of users to any type of examination and the use of service;

c) Advising on hiring its services;

d) Professional judgments on the evidence that shall be presented to any legal jurisdiction;

e) Updating the users on any update on their agreement with the digital forensic laboratory.

4.4.2.8 The resolution of the laboratory complaints

In the manner of handling complaints, the digital forensic laboratory shall ensure the existence of documented procedures for handling electronically the complaints of the laboratory customers, personnel, or any other party involved in the provided services.

The complaints shall be closed with the existence of the following information:

a) A reference number;

b) A dated and timed history from the creation to the closure including any action made to the ticket;

c) The contact information of the reporter unless the reporter requests to be anonymous;

d) The assigned personnel to assess the complaint;

e) The personnel who was the complaint referred to in order to be resolved;

f) If the complaint or feedback is regarding a technical axis of the digital forensic laboratory services, the services shall be stated within the complaint information;

g) The action or feedback that been made to resolve the complaint.

Unless the complaint reporter requested to be anonymous, a documented procedure of its communication regarding any feedback on a complaint with the reporter shall be completed.

4.4.2.9 Identifying and controlling nonconformities

In the QMS, the existence of a procedure for handling the identification and management of nonconformities at any part of that system shall be completed. The following shall be satisfied by the procedure:

a) Appointing the responsibilities and accountabilities of handling the nonconformities;

b) Actions are taken immediately;

c) If necessary, the digital forensic laboratory examinations shall be halted along with any non-approved report;

d) A description of the scope of the determined nonconformity;

e) Each nonconformity case shall be documented and registered in a register for a pre-identified period of time for further analysis and quality improvement if required;

f) Appointing the responsibilities of personnel and process of the resumption of the examinations.

All the above responsibilities and accountabilities shall be reflected in the digital forensic laboratory RAM and any update on the roles shall be recorded immediately.

A pre-defined procedure shall be completed to evaluate whether to hold the examinations and the non-approved reports.

4.4.2.10 The actions of correction

In the case of any non-conformities, immediate corrective action shall be performed by the digital forensic laboratory. Any corrective action shall be implemented only to eliminate or eradicate the root cause of non-conformities to avoid any implication that may or may not affect the quality of the provided services. If any nonconformity case arises, a pre-defined procedure shall be taken in order to handle nonconformities lifecycle; this includes but is not limited to:

a) Nonconformities review;

b) Analyse the situation to determine the root cause;

c) Analyse any non-direct implication caused by the nonconformities;

e) Evaluate the requirement of corrective action(s);

f) Plan for corrective action(s), including appointing responsibility and accountability for any corrective activity;

g) Appoint personnel to follow up and coordinate any communication regarding this action, with the authority to escalate to any level to ensure the implementation of the action;

h) Record the result of the corrective action;

i) Evaluate the effectiveness of the corrective action

j) Record and documented the resolution in an electronic database system for future purposes.

The digital forensic laboratory shall ensure the availability of the recorded and documented resolutions to the relevant level of personnel. The level of personnel, which have access to any case resolution, shall be pre-defined.

4.4.2.11 The actions of Prevention

In the case of any potential nonconformities, an action(s) shall be performed by the digital forensic laboratory to eradicate or eliminate the causes and to prevent the occurrence of the identified potential nonconformities.

A documented procedure shall be put in place by the digital forensic laboratory to handle potential causes that may result in nonconformities cases; this includes

but is not limited to:

a) Identify potential causes through the analysis of the data of the digital forensic laboratory;

b) Evaluate the situation with the required preventive action to eliminate these potential causes;

c) Review the result of the analysis to determine whether to be considered as potential causes or not and determine the root cause;

d) Plan for preventive action(s), including appointing a responsibility and accountability for any preventive activity;

e) Appoint personnel to follow up and coordinate any communication regarding this action, with the authority to escalate to any level to ensure the implementation of the action;

The digital forensic laboratory shall ensure the availability of the recorded and documented resolutions to the relevant level of personnel. The relevant level of personnel, which have access to any case resolution, shall be pre-defined.

4.4.2.12 Continuous improvement

The digital forensic laboratory shall ensure the existence of an effective continuous improvement process in its QMS including any activities related to the examination of the evidence through the digital forensic laboratory management review. This review shall be planned to evaluate the digital forensic laboratory performance. A risk assessment shall be performed to prioritise the improvement activities and the activities shall be planned, implemented and documented in accordance with that priority. The risk assessment shall include the effort and benefits dimensions, where financial, human and equipment resources, effort, and the business involvement shall be considered and prioritizing for the improvement. The process of the continuous improvement of the QMS shall be evaluated through the digital forensic laboratory internal audit.

4.4.2.13 Control of records

The digital forensic laboratory shall ensure the existence of a process allowing technical and quality records to be identified, collected, indexed, accessed, stored, maintained, amended, and disposed of safely. The records shall include, at least, the

following:

a) A list of laboratory suppliers and evaluation of the suppliers' performance;

b) Staff academic qualification, training, professional certification and any relevant information related to the staff;

c) Examinations requests;

d) A record of all report from a referral laboratory;

e) A record of all the evidence that been accepted for examinations;

f) Information regarding any materials, equipment, and procedure involved directly or indirectly with the digital forensic laboratory examinations;

g) A record of the chain of custody of any accepted digital evidence for examinations;

h) A record of the examinations' documentations (e.g. the used methods, notes, hashing information, information regarding the failure of matching the evidence hashing... etc.);

i) Official examinations reports;

j) incident and accident records and any taken action;

k) Nonconformities cases and any related information (e.g. planned action, plan implementation, and final report);

l) Preventive cases and the taken action;

m) Complaints and any related information;

n) Performed and planned internal and external audit;

o) Performed and planned quality improvement activities;

p) Management review (see 4.4.2.15);

q) Information related to any case presented to the legal justice system (e.g. evidence presentation report);

r) All minutes of meetings regarding the QMS;

s) All external audit documents;

t) Output of the management review process and any relevant documents;

u) Reports of the digital forensic laboratory' environmental violation (see 4.5.2);

v) The digital forensic laboratory equipment and software information (see 4.5.3.4.6);

w) Documentation of preformed examination applied to digital evidence (see 4.5.4.5).

4.4.2.14 Evaluation and audits

The following subsections cover the requirements of the evaluation and audits of the digital forensic laboratory; audits include internal and external audits. The subsections present the requirement to establish a process to review the suitability of the digital forensic laboratory procedures. In addition, the requirement of user feedback and the staff suggestions are covered. Later, the requirement of the establishment of a documented risk assessment process, and quality performance indicators are presented.

4.4.2.14.1 The general requirements of the evaluation and audits

A process shall be established by the digital forensic laboratory to evaluate and audit the QMS. The process output shall demonstrate all the lifecycle of the examination and any supportive process in order to ensure the conformity of the system.

4.4.2.14.2 The review of the digital forensic laboratory procedures suitability

The digital forensic laboratory shall ensure the existence of a process to evaluate the authorized personnel who are professionally qualified to perform the examination using the equipment or/and software. This process shall ensure their up to date skill in using the equipment correctly to ensure the accuracy of results. This process shall also review the latest technology in the field that may increase the accuracy of the results. This shall be compared to the digital forensic laboratory requirements to perform the required examinations.

4.4.2.14.3 The user feedback and assessment

The digital forensic laboratory shall be establishing a channel and seek for the users' feedback to ensure that the provided services met the expectation and requirements of the user. Thus, the digital forensic laboratory shall ensure the confidentiality of the users' feedback to enable the enhancement on its services. A record of any feedback including the taken action(s) shall be kept and analysed, for service improvement purposes.

4.4.2.14.4 The employees' suggestions

The digital forensic laboratory shall enable its employees to provide any suggestion that should enhance services directly or indirectly. All suggestions shall be accepted, evaluated, actioned, and recorded. The digital forensic laboratory staff suggestions shall be taken confidentially if requested and the digital forensic laboratory shall ensure that any suggestion and action does not affect the suggester negatively directly or indirectly.

4.4.2.14.5 The internal audit of the laboratory

The digital forensic laboratory shall plan and conduct an internal audit annually to inspect whether the QMS of the digital forensic laboratory, including pre and post examination stages, has effectively sustained the requirements of the designed system. The digital forensic laboratory shall ensure that certified personnel in assessing all the levels of the QMS, only conduct the audits. Any audit shall be documented from planning until finalizing the report. All the responsibility and authorities of the audit personnel shall be added to the digital forensic laboratory RAM and updated immediately when a change occurrs (see 4.4.2.13). When a nonconformity case is identified within the audit, immediate action has to be taken by the auditor(s) to escalate the case to the correct level of management in order for management to plan and implement corrective action(s) (see 4.4.2.10).

4.4.2.14.6 Risk management

The digital forensic laboratory shall establish a documented risk assessment process to evaluate any factor that may affect the main mission of the digital forensic laboratory or any activity related to any stage of the digital forensic laboratory examinations. This evaluation shall be extended, if a potential failure is identified, to the plan and implement action(s) to eliminate the cause of that failure.

4.4.2.14.7 The laboratory quality performance indicators

The effectiveness of the QMS shall be ensured by the digital forensic laboratory, and evaluated through the establishment of quality performance indicators. The

evaluation shall include the entire lifecycle of the examinations and any supportive process that interact with the system. Indicators shall be able to evaluate the QMS through the number of activities that have not been performed correctly, or resulted in failure (e.g. number of unacceptable results, number of hashes not matching cases of the cloned data evidence with hash of the original version). A periodical review shall be performed, at least once a year, to ensure the appropriateness of the indicators to the QMS.

The monitoring of the indicators shall be carried through a pre-defined process. The process shall include, at least, the objectives, methodology, interpretation, limitation, recommendations, and time duration of the measurement execution.

4.4.2.14.8 External audit

In the case of the appearance of nonconformities or potential nonconformities cases in an external audit, the digital forensic laboratory shall ensure that, an action is processed immediately for corrective or preventive action (see 4.4.2.10 and 4.4.2.11). Any record of the external review and related activities shall be documented and stored (see 4.4.2.13).

4.4.2.15 Management review

The following subsections cover the requirement of establishing a review process by the digital forensic laboratory management to ensure the appropriateness, adequacy, and effectiveness of the digital forensic laboratory QMS. These subsections cover the input, activities, and output of the process.

4.4.2.15.1 The management review general requirements

The QMS shall be reviewed periodically by the digital forensic laboratory management, to ensure its appropriateness, adequacy, and effectiveness to requirements. This is in order to ensure that the provided services meet the service agreement.

4.4.2.15.2 Review input process

The process of the management review shall ensure the following input are

considered, at least, when a review is performed:

a) Review of the digital forensic laboratory procedures periodically (see 4.4.2.14.2);

b) The used feedback and assessment (see 4.4.2.14.3);

c) Employees' suggestions (see 4.4.2.14.4);

d) Internal and external audit (see 4.4.2.14.5 and 4.4.2.14.8);

e) Risk management (see 4.4.2.14.6);

f) Quality performance indicator (see 4.4.2.14.7);

g) Responsibility, accountability and interrelationships (See 4.4.1.2.5);

h) Communication (see 4.4.1.2.6);

i) The report of any failure on the output of (4.4.2.5.2);

j) The selection, evaluation and approval approach of (4.4.2.6);

k) The result and report of any failures in personnel competency assessment that require further action of retraining or else (see 4.5.1.6);

l) Result and reports of the continuous improvement (see 4.4.2.12);

m) Effectiveness of the process of the control of records (see 4.4.2.13);

n) Follow up or previous of the planned actions on the previous management reviews;

o) Evaluation report on the level of management commitment (see 4.4.1.2.1).

p) Any element or factor that may affect the effectiveness of the QMS.

q) Failure cases of complaints resolution (see 4.4.2.8);

r) Business Continuity Management (BCM) reports (see 4.4.2.16).

4.4.2.15.3 Review process activities

The input information shall be analysed as part of the management review to search for information that identifies any point for a failure in a process that could be modified, and enhanced; this is considered as part of (4.4.2.11). The activities of the review shall be extended to enhance the digital forensic laboratory QMS, including and supportive activity to the system. Any planned action shall be followed-up by appointed personnel with the authority to escalate to any level to ensure the implementation of the action and to avoid deviations. An update on the follow-up on the planned action shall be reported in the following management reviews.

4.4.2.15.4 The output of the review process

The review output and any relevant documents shall be recorded (see 4.4.2.13); this process shall include, at least:

a) Modification and enhancement on the QMS;

b) Activities related to the need for the digital forensic laboratory resources;

c) Activities related to the enhancement of the digital forensic laboratory services;

d) Activities related to the supportive processes.

The appointed personnel to follow-up the planned action shall be responsible for any deviation, with the full accountability of any failure on the digital forensic laboratory management.

4.4.2.16 Business continuity management

The digital forensic laboratory shall establish a Business Continuity Management (BCM) system. This includes but is not limited to:

a) Information Technology Disaster Recovery (IT DR) program management;

b) BCM policies;

c) Business risk assessment;

d) BCM governance framework;

e) Monitoring procedures;

f) Internal audit procedures;

g) Performance evaluation metric;

h) Continual improvement process;

The digital forensic laboratory shall ensure that the laboratory business continuity is planned to extend the physical and virtual property of the laboratory. In addition, the BCM system shall be tested periodically.

The digital forensic laboratory shall establish a training and awareness programme for all its personnel, and should ensure any changes are evaluated to avoid business disruption. It shall ensure the continuity of the business and the evidence storage security. The BCM reports shall be reviewed periodically by the management, and an emergency meeting shall be called when necessary (see 4.4.2.15).

4.5 TECHNICAL REQUIREMENTS

The technical requirements have been covered in this section through a various number of subsections. The first subsection covers the requirements of the digital forensic laboratory personnel and this subsection covers the personnel training, education, competence assessment and performance, job description, and records. In addition, the section covers the requirements of the digital forensic laboratory environmental conditions and laboratory operation, which include the evaluation, acceptance, establishment, and management of the cases. Also the handling, preservation, disposal, and presentation of digital evidence. This section also focuses on the core of digital forensic laboratories which is the examination requirements. The examination subsection gives the requirements for strategy, preparation, discovery, investigations, documentation, and reporting of the digital forensic laboratory examinations.

4.5.1 Personnel

The following subsections present the requirements for the digital forensic laboratory personnel.

4.5.1.1 General requirements

All the personnel management and records shall be processed by a document procedure, and the digital forensic laboratory shall ensure the establishment and maintenance of this procedure.

4.5.1.2 Qualifications and professional certifications

The digital forensic laboratory shall establish the required qualifications academically and professionally and the required experience for each position and level. The qualification and experience shall be demonstrated based on the required skills and knowledge that are required to perform the job and tasks. The personnel who perform any technical activity shall be certified theoretically and practically for the assigned task.

4.5.1.3 The laboratory job descriptions

A documented job description for all the roles in the digital forensic laboratory have to be established. Each job shall have a different level based on the experience required and each level shall have a variety of responsibilities. The responsibilities of each job shall be reflected in the digital forensic laboratory RAM (see 4.4.1.2.5).

4.5.1.4 Personnel introduction to the digital forensic laboratory

Any new employees at any level shall be enrolled in a programme introducing the following, at least:

a) The digital forensic laboratory general information (e.g. brief history, hierarchy, mission, and the provided services);

b) The digital forensic laboratory facilities, including the safety and security instructions;

c) The team or the department that the employee is going to contribute in and his/her superior, including their information (e.g. names, emails, job titles, and contact numbers);

e) The job description, tasks, performance indicators for the assigned job;

f) Work protocols;

g) Work rights from/to the organization and employee;

The digital forensic laboratory shall have documented evidence of providing a copy of all the elements of the programme sent to the new staff;

h) the processes, procedures and policies of the security in the laboratory.

4.5.1.5 Education, training and professional development

The digital forensic laboratory shall ensure the establishment and enablement of a programme focused on continuous education and professional development across all levels of staff. The programme shall focus on developing the staff on each assigned task or any related development, which shall enhance the quality of the digital forensic laboratory services. The digital forensic laboratory shall ensure that the personnel receive training on the following areas, at least:

a) Assigned tasks;

b) The digital forensic laboratory QMS;

c) Organizational procedures (e.g. safety procedures and hierarchy protocols);
d) Rules of information privacy and confidentiality;
e) The digital forensic laboratory processes and procedures;
f) The digital forensic laboratory electronic systems, if applicable.
The digital forensic laboratory shall have document evidence of its personnel receiving the training.

The digital forensic laboratory shall ensure the establishment and maintenance of a Training Manual (TRM). The TRM should contain the digital forensic laboratory procedures of the establishment of the required technical knowledge, skills, and abilities for technical personnel to attain a level of competency thereby enabling them to be certified by the digital forensic laboratory management to perform technical services. The digital forensic laboratory should provide the appropriate training for examiners to maintain their certifications through proficiency testing and to provide opportunities for advanced certifications to perform more complex technical, and administrative tasks. The TRM shall be an extension of the QM (see 4.4.2.2.2).

4.5.1.6 Competence assessment

The digital forensic laboratory shall assess each of the personnel based on pre-identified performance indicators, including soft skills. The assessment shall cover the technical and managerial personnel. The assessment can be performed in a direct way and/or an indirect way with a tangible measurement. This includes but is not limited to:
a) Direct observation;
b) Analysis of the examination results;
c) Audited records;
d) Problem-solving skills assessment;
e) The number of corrective actions resulted from the personnel performance.
The assessment shall be performed periodically, at least once a year, and retraining action shall be reviewed (see 4.4.2.15.2) and actioned for retraining or quality improvement.

4.5.1.7 The employees' performance reviews

The digital forensic laboratory shall ensure reviewing the performance of its employees periodically to ensure the quality of the performed tasks. The result of the review shall be sent to the management review if any further action is required (see 4.4.2.15).

4.5.1.8 Personnel records

The digital forensic laboratory shall ensure they hold personnel records including, at least, education, training, previous experience, licenses, performance evaluation reports, legal identify (e.g. National identification or passport), current jobs, job description, accidents and occupational hazards, competency assessments, and achievements.

4.5.2 The Environment of The Digital Forensic Laboratory

The following subsections articulate the requirements of the environmental conditions of the digital forensic laboratory including the facilities.

4.5.2.1 The Environment General Requirements

Allocated facilities have to be designated by the digital forensic laboratory to perform the examination that is designed as part of the provided services. The suitability and adequacy of the allocated facilities by the digital forensic laboratory to the preformed examinations is to be assured.

4.5.2.2 The Digital Forensic Laboratory and Its Office Facilities

The facilities of the digital forensic laboratory shall be secured physically with an access control system (for more information, see BS EN ISO/IEC 27002:2017 Clause 9.2.3; BS EN ISO/IEC 27001:2017 Clause 6.1.3 and Appendix A.11.1.2).
The digital forensic laboratory shall establish a documented access control process with its human resources processes to ensure the creation and closure of any access within the hiring and termination process. It shall also ensure only authorized personnel have access to a certain zone, for instance, examiners only can have

permanent access to the examinations space. The digital forensic laboratory shall ensure the existence of a documented procedure to control access to the digital forensic laboratory system, and its appendices. The access control shall be reviewed, and maintained when any change related to the personnel occurs. The access control records shall be added identified, collected, indexed, accessed, stored, maintained, amendment, and disposed of safely (see 4.4.2.13).

4.5.2.3 Staff facilities

The digital forensic laboratory shall ensure the access of its personnel to sufficient facilities, at least: washrooms, drinkable water, protective equipment storage. All of these facilities, shall not be within the digital forensic laboratory examination room(s).

4.5.2.4 The environmental conditions

The digital forensic laboratory shall ensure its facilities are cleaned regularly, and all the facilities shall be maintained when it is required. The digital forensic laboratory shall ensure its environmental conditions, including recording and investigating, any suspected violation of the environmental condition that might or might not affect the evidence.

The digital forensic laboratory shall have a documented procedure to handle any environmental violation suspicion, such as electromagnetic interference, electrical supply, humidity, radiation, and high temperature, which would affect the quality of the digital forensic laboratory examination adversely. It shall ensure the existence of precautions for handling physical devices and hazardous materials; for instance, electricity, and sharp edges. All the investigations shall be recorded (4.4.2.13) and controlled. The digital forensic laboratory shall ensure immediate action is performed to solve an environmental violation. Reports of the violations, shall be reviewed by the management (see 4.4.2.15). Also it shall ensure the effective separation between its sections, which assure the prevention of interference between the electronic evidences.

4.5.3 The Digital Forensic Laboratory Operation

The following subsections cover the digital forensic laboratory operational requirements; including handling new cases when evidence arrives, and evaluating the situation to accept a case. In addition, evidence management is covered as it plays a significant part in the operation, which focuses on the procedures of handling the evidence and storing them.

4.5.3.1 General requirements

The digital forensic laboratory shall ensure the existence of documented procedures of its operation including but not limited to:

- Case file management
- Control and performance of the digital forensic laboratory equipment and software
- Evidence management

4.5.3.2 The case file management

The digital forensic laboratory shall ensure the existence of a documented procedure to handle cases files. The digital forensic laboratory shall ensure that all its technical records are recorded, and stored securely in a Digital Forensics System (DFS). The DFS contains the official records of a request of the customer's services and the digital forensic laboratory response to requested services. The technical records in the DFS shall include the technical and quality records for each examination or service request. The digital forensic laboratory shall include events of the case in its repositories chronicle from the initiation through to the case closing and disposition. The digital forensic laboratory shall ensure the existence of a documented procedure to establish a new case. In addition, it shall ensure to have a predefined metrics to determine the priority of the new case. The digital forensic laboratory shall ensure the following information, at least, are included in the case file folder:

a) Original service request and background documentation;
b) Evidence information, including the time and date of collection;
c) Evidence Chain of Custody (CoC) (see 4.5.3.6.2);
d) Communications (written and summary of oral communications);

e) Technical notes of procedures performed during imaging and analysis of evidence.

f) Report(s)

g) Quality documents (e.g. technical and administrative review forms) Also any profile creation or amendment shall be stamped electronically with the personnel, time, and date.

4.5.3.3 Case evaluation and acceptance

The digital forensic laboratory shall ensure the existence of a documented procedure to evaluate and establish new cases. Unless there is a need for amendment, the digital forensic laboratory shall have a default Service Level Agreement (SLA), to be applied directly during the initiation of a case. The digital forensic laboratory shall ensure the existence of a documented procedure to handle the status of the case, accepted or rejected, and the required communications shall be performed when the decision is made. A copy of the SLA shall be sent to the legal body of the digital forensic laboratory for scrutiny.

The digital forensic laboratory shall ensure the existence of a documented procedure for accepting the evidence. The digital forensic laboratory shall ensure that the acceptable evidence is isolated, secured, and preserved in the state of the evidence digitally and physically (see 4.5.3.8). To guarantee the integrity of the evidence, the digital forensic laboratory should encourage or require the collection of evidence at the scene for presentation to a court of law, in accordance with the mapped processes from several digital forensics International Standard clauses. The mapped processes can be seen in Appendix B. The digital forensic laboratory shall ensure to include a declaration in the reports of the cases declaring the status of the knowledge of the digital forensic laboratory on the acquisition and transportation processes of the evidence at the scene in accordance with accredited International Standards.

If a case is accepted, the digital forensic laboratory shall ensure the following conditions, at least, are met:

a) The CoC record is up to date;

b) The collected evidence information is entered in the case information;

c) Pictures of the evidence are added to the case profile;

d) Evidence is entered, numbered, and labelled, in the inventory management system;
e) A detailed check on the evidence to ensure no damages have occurred (e.g. bag or seals opened).

4.5.3.4 The digital forensic laboratory equipment and software

The following subsections cover the acceptance, maintenance, and records of the equipment and software of the digital forensic laboratory.

4.5.3.4.1 The equipment and software general requirements

The digital forensic laboratory shall ensure the existence of a documented process to handle selecting, evaluating, purchasing, and managing the digital forensic laboratory equipment and software. The process shall cover equipment and software that are required to perform activities in the scope of the digital forensic laboratory (see 4.4.1.1.2). The following are common examples of the digital forensic equipment:
a) Forensic workstations and forensic laptops;
b) Video analysis workstation;
c) Mobile data extraction equipment;
d) Write blockers;
e) Disk duplicators;
f) Drive and data wiping devices;
g) Forensic software used for imaging, wiping, and data recovery.

The digital forensic laboratory shall ensure the existence of the required equipment and software resources required to provide its services (see 4.4.2.1). The digital forensic laboratory shall ensure the maintenance of its equipment and software, including replacing it if necessary, in the case of equipment, to ensure the quality of its services. The digital forensic laboratory software is either independent software of embedded software in equipment.

4.5.3.4.2 The acceptance of the equipment and software

The digital forensic laboratory has to verify that the used equipment and software

is correctly installed and meets the necessary performance to perform the required tasks. This procedure shall be executed during the installation of equipment and software, before the first use, and when the equipment is moved, or the software is reinstalled. For acceptance, the digital forensic laboratory shall ensure that all of its examination equipment and software has an information record (see 4.5.3.4.6).

4.5.3.4.3 Equipment and software under operation

Any accepted equipment or software by (4.5.3.4.2) is considered as equipment and software under the digital forensic laboratory operation. The digital forensic laboratory shall ensure that accredited, authorized, and trained personnel operate all of its equipment and software. The instructions of the digital forensic laboratory equipment and software shall be available at all times to the technical personnel, with no approval required, under the equipment and software information (see 4.4.2.13 and 4.5.3.4.6) including but not limited to the operation, installation, safety, maintenance guideline, and any relevant manuals.

4.5.3.4.4 The maintenance and repair of the equipment and software

The digital forensic laboratory shall establish its programme to ensure the prevention of unnecessary maintenance through following the equipment manufacturer's instructions for installation, movement, operation, and storage. This programme shall be documented, and clearly communicated to the personnel. The documentation shall be included with the equipment information records to be accessed at any time. The digital forensic laboratory shall ensure the existence of a documented procedure on the maintenance of its software and equipment, including but not limited to:

a) Reporting the needs for maintenance;

b) Validate the requirement of the maintenance;

c) Approval of the maintenance.

The digital forensic laboratory shall ensure specifying the impact of the maintenance or repair on its current examinations. The specialized personnel shall be informed in case the impact of the maintenance extends to break the service agreement (see 4.4.2.4). A corrective action shall be performed to avoid such a case (see 4.4.2.10). In the case of software maintenance, including updates and upgrades,

approval of the digital forensic laboratory manager shall be obtained. The digital forensic laboratory shall ensure the existence of a documented procedure in the case of software update or upgrade including but not limited to:

a) Compare the result of an examination of a piece of evidence between the old and new version;

b) Task approval;

c) Validity of the upgrade or update to the performance of the digital forensic laboratory;

d) Validity of the reason for the upgrade or update.

4.5.3.4.5 Reporting equipment and/or software incident

The digital forensic laboratory shall ensure the existence of a documented procedure for reporting a software and/or equipment incident. The digital forensic laboratory shall have a documented procedure to seek support from hardware and software manufacturers. The digital forensic laboratory shall ensure to appoint a single point of contact to communicate with manufacturers, where only that delegated person is authorised to communicate with manufacturers. The digital forensic laboratory shall perform an investigation after each incident resulting in a report. The report shall contain the root cause if founded and the manufacturer shall be informed. Also, if the case has resulted from the digital forensic laboratory operation, the laboratory shall ensure to consider a prevention plan for the future in the equipment or software prevention programme (see 4.4.2.11). in addition this shall be added as a learning lesson recorded under the equipment and software information for future prevention (see 4.4.2.11).

4.5.3.4.6 Equipment and software information record

The digital forensic laboratory shall have an equipment and software information record (see 4.4.2.13) and this record shall be identified, collected, indexed, accessed, stored, maintained, amendment, and disposed of safely. This record shall include but not limited to:

a) Any equipment or software shall have a unique identification code;

b) Each item in the equipment or software shall have a sub unique identification code;

c) Manufacturer information, including contact details;
d) History record, including the acceptance date and time and the maintenance details;
e) Information of the personnel dealt with the equipment or software (e.g. detail of the personnel who accepted the equipment);
f) A copy of the initial request of purchases;
g) Financial information (e.g. cost of purchases, cost of maintenance, and cost of repair parts);
h) Manufacturer's manual and instructions;
i) Physical location;
j) Movement history, including date, time, reason for movement, copy of the movement approval, personnel who moved it;
k) Any related information required for operation or termination stages.

4.5.3.5 The digital forensic laboratory consumables

The digital forensic laboratory shall ensure the existence of a documented procedure for defining the need, evaluating offers, purchasing, acceptance, and storage of the consumables of the digital forensic laboratory.

4.5.3.6 Evidence Management

The following subsections cover requirements of the management of the digital evidence including the CoC and evidence storage.

4.5.3.6.1 Evidence management general requirements

The digital forensic laboratory shall ensure the existence of documented procedures to handle physical and logical digital evidence, this includes the collection of Electronically Stored Information (ESI) from a networked environment. It shall ensure that the examined evidence are documented, and tracked in the case file folder, and DFS. The digital forensic laboratory shall have a system of evidence management. This system shall be able to provide an audit trail of evidence from the time it is received or collected in the digital forensic laboratory until it is

returned to the customer, or disposed of, as applicable. There shall be no unaccounted time in the audit trail.

The digital forensic laboratory shall ensure the existence of a documented procedure for damaged physical-digital evidence. The digital forensic laboratory shall ensure the existence of a documented procedure to handle evidence delivered by courier on arrival. This includes, but is not limited to:

a) The evidence is unpacked and visually inspected by technical personnel to ensure only those items that will be examined are accepted into evidence control;

b) Only physical-digital evidence is logged, unless the non-digital evidence is unique and required to facilitate the examination;

c) The original evidence is visually examined for damage.

The digital forensic laboratory should immediately resolve any discrepancies regarding the package contents with the customer. The digital forensic laboratory shall provide photographs of any damaged evidence immediately followed by a written report to the customer; this report shall be recorded to the case file.

The digital forensic laboratory shall ensure the existence of a documented procedure to seal and label evidence in a protective method. The digital forensic laboratory shall ensure the existence of a documented procedure to unseal evidence in a protected method. The digital forensic laboratory shall ensure the existence of a documented procedure to control the extracted data, and shall ensure that the original digital data are being protected from change during the imaging or previewing processes.

4.5.3.6.2 Evidence Chain of Custody

The digital forensic laboratory shall ensure the existence of a documented procedure to handle the Chain of Custody (CoC) of the digital evidence. The evidence CoC is complied with the DFS and the case file management systems (see 4.5.3.2); stored in the DFS. The following personnel shall be included, at least, in any CoC record:

a) Transactions (e.g transfer from person to person or storage or removal of evidence in the evidence facility);

b) Evidence custodian;

c) Digital forensic analyst (who imaged and analyzed it);

d) The owner of the evidence;

e) Participants in processing the case;

f) Anyone else involved in the CoC processes;

g) Physical evidence unique identifier.

The CoC record shall be controlled (4.4.2.13) and the access to it shall be controlled via (4.5.2.2) where only privileged personnel view the record and any amendment shall be monitored and approved by a superior. The evidence has to be photographed before and after. Any CoC record shall have the following, at least:

a) Date and time of the record creations and any amendments;

b) Record creator or who action amendment;

c) The details of the characteristics of the preserved evidence (e.g. type and size of the hard drive);

d) Evidence gathered methods details (input from the First responder);

e) Examination method details;

f) The unique identification of the evidence;

g) Digital forensic tool details, including the version number;

h) Pictures of the evidence when the evidence is handed to other personnel;

i) Picture of the evidence while checked in if it is not data;

j) Unique property number in the digital forensic laboratory secured storage;

k) The case number;

l) The case details (e.g. if this evidence is required to be presented to the court of law later of not);

m) Linked digital evidence if it exists;

n) Techniques that have been used to ensure the integrity of the evidence (e.g. Checksum Redundancy Check, timestamp, and watermarking).

The digital forensic laboratory shall ensure the specialized personnel specify all the details of the preserved evidence (e.g. when a personal computer is been preserved, all the internal components shall be detailed in the CoC record including but not limited to the type, size, manufactured company of the Random-access memory, Hard drive, Motherboard, computer' case, and CD driver). The digital forensic laboratory shall ensure the establishment of a defined process to handle the evidence, including if the evidence is been compromised or the integrity has been violated in any way.

4.5.3.6.3 Evidence Storage

The following subsections present the requirements for storing physical and digital evidence. In addition, how the digital forensic laboratory shall ensure the integrity of the evidence within the storage.

4.5.3.6.3.1 General requirements

The security of digital forensic evidence extends to two types of storages: physical and virtual (digital). Both types shall be included and secured within the access control (4.5.2.2) to ensure the integrity and security of the digital evidence. The digital forensic laboratory shall have a documented procedure to process, store, control, document, and secure the evidence. It should process digital evidence (physical and virtual) systematically; and, the system should be able to provide an audit trail for the collection of digital evidence and documents from the source. It should be able to establish a record that the data is collected correctly and was not altered, modified, and/or contaminated.

The digital forensic laboratory shall have a procedure to reseal the evidence after accepting it and placing it in the evidence safe, until assigned to an examiner for imaging, examination, or other technical processes. The digital forensic laboratory shall have a procedure of returning original and/or derivative evidence to the customer sealed and secured. The digital forensic laboratory shall ensure that the storage ensures the continuing integrity of the laboratory documents, records, equipment, material, consumables, digital evidence (data), and the physical-digital evidence.

4.5.3.6.3.2 Physical-digital Evidence

The digital forensic laboratory shall ensure the full segregation of the storage physical-digital evidence and the other stored items. The digital forensic laboratory shall ensure that stored physical-digital evidence is preserved in a suitable temperature and humidity to ensure the integrity of the evidence. Each physical-digital device that has a radio transmitter has to be ensured by the digital forensic laboratory that it is preserved in a faraday-shielded area. The digital forensic laboratory shall ensure the existence of a documented procedure to store temporary

physical-digital evidence, when technical processes are finished and waiting for administrative processes. In addition the digital forensic laboratory shall ensure that the assigned examiner is the only personnel who has access to the temporary storage. The digital forensic laboratory shall ensure to appoint delegated personnel to manage the laboratory secure physical storage and its inventory management system.

4.5.3.6.3.3 Digital (virtual) Evidence

The digital forensic laboratory shall have secure data storage for managing the digital forensic laboratory data, and to store the preserved data evidence. It shall ensure the full segregation between the systems handling the laboratory data and the evidence data. The digital forensic laboratory shall ensure the full segregation of the storage virtual-digital evidence and the other digital (data) items. Access to laboratory data management systems, shall be controlled (see 4.5.2.2). The digital forensic laboratory shall have a documented procedure to handle digitally stored evidence off the storage area network to perform analysis on an archived service request or as part of the audit. In addition, it shall ensure the deployment of its storage infrastructure using but not limited to the following storage technologies:

a) Redundant Array of Independent Disks (RAID);

b) Virtual and physical backups;

c) Replications to support BCM;

d) Continuous Data Protection (CDP);

These storage technologies shall not be part of the storage security controls. (see BS EN ISO/IEC 27040:2016 Clauses 5.2 and 7.3.3 and sub-clause 6.8.1.3).

The digital forensic laboratory shall have strict access control on the virtual storage, for either evidence or access. The authorities for each personnel level have to be approved by the director. The virtual storage management shall be completely internal accessed with restrictions on any external access. Monitoring, managing, and auditing procedures shall be established and authorised to perform its security role. The digital forensic laboratory shall have a process of data confidentiality policies. regarding its virtual storage. Any guaranteed access to personnel shall be associated with an acknowledgement of the personnel, to the digital forensic laboratory data confidentiality policies.

4.5.3.7 The disposal and preservation of digital evidence

The digital forensic laboratory shall ensure the existence of a documented procedure to preserve the evidence physically and virtually after examination in secured storage (see 4.5.3.6.3). The digital forensic laboratory shall preserve evidence under certain conditions that including but are not limited to:

a) Awaiting for collection by the customer or else;

b) Awaiting a hearing in the court of law;

c) If it is required for the second turn of examination;

d) To pursue the examination later.

The physical and virtual secure storage of the evidence shall be segregated completely from the digital forensic laboratory secured storage which contains the digital forensic laboratory equipment and consumables (physical) or the Information Technology (IT) infrastructure which manage the laboratory systems (virtual). The time of preservation varies from a case to another; thus, the digital forensic laboratory shall evaluate and define the time required according to the need. Unless the original evidence is not returned for specific purposes, for instance by a court of law order, the digital forensic laboratory shall have a pre-defined retention period of original and/or derivative evidence.

The digital forensic laboratory shall have a documented procedure on wiping digital media securely and completely delete digital data. The data shall be rendered unrecoverable by reasonable means, including through forensic methodologies. Digital media that cannot be wiped may be destroyed through the sanitization procedure. The digital forensic laboratory shall ensure the existence of a documented procedure to sanitize digital evidence that requires sanitization (for more guidance on the data sanitization technologies, see BS EN ISO/IEC 27040:2016 sub clause 6.8.1).

The digital forensic laboratory shall ensure it has a procedure for consumables disposal safely. It shall ensure the existence of a documented procedure to prepare evidence for preservation, including but is not limited to:

a) Bagging, sealing, and packaging the evidence (see ISO 27037 Sub-clause 6.9.3);

b) Transporting the physical evidence to the digital forensic laboratory secure storage in accordance with applicable points of (ISO 27037 Sub-clause 6.9.4).

c) Update the case record.

4.5.3.8 Evidence presentation

The digital forensic laboratory shall ensure the existence of a documented procedure to handle original or/and derivative evidence that is required to be presented in the court of law. The digital forensic laboratory shall comply in presenting evidence with the rules of evidence code of the jurisdiction, as it varies from a country to another. Unless it is not required by jurisdiction, the digital forensic laboratory shall ensure the existence of a documented procedure to provide a statement of the authenticity of the evidence. The digital forensic laboratory shall add the first responder actions to the statement, which has been performed before arriving at the digital forensic laboratory. This includes but is not limited to:

a) Digital evidence handling identification method;

b) Digital evidence prioritization at the scene;

c) Collect and acquire method;

d) Digital evidence packaging procedure;

e) Digital evidence transportation procedure.

The digital forensic laboratory shall ensure, its staff, attend and testify regarding the evidence that they examine, validate, prepare and related activities if required by the jurisdiction. If the court of law has requirements for expert or evidentiary witness, the digital forensic laboratory shall ensure to apply that requirement when laboratory staff are called to be a witness. The digital forensic laboratory shall comply with the jurisdiction of all digital evidence handling procedures, as it varies from one jurisdiction to another. The digital forensic laboratory shall have a documented digital redaction techniques procedure (see ISO/IEC 27038:2014).

4.5.3.9 Operation manual

The digital forensic laboratory shall ensure the establishment and maintenance of an Operation Manual (OM), which this manual includes but is not limited to:

a) Evidence management;

b) Equipment control;

c) Equipment and software performance verification;

d) Case file management system.

The OM shall be an extension of the QM (see 4.4.2.2.2).

4.5.4 Examination

The following subsections present the requirements that the digital forensic laboratory shall take into consideration for its examinations. This includes the strategy, preparation, discovery, investigations, documentation, and reporting of the digital forensic laboratory examinations.

4.5.4.1 Examination General requirements

The digital forensic laboratory shall ensure the existence of a documented format of its technical procedures. The control, and version, are maintain in accordance with document controls (see 4.4.2.3). The format for the technical procedures shall include at least the following;

a) Purpose;

b) Scope;

c) Software/equipment;

d) Unique definitions per procedure;

e) Limitations;

f) Procedures;

g) References

h) Notes;

i) Safety.

Laboratory management shall officially approve the technical procedures. The digital forensic laboratory shall have a procedure for handling known and unknown files. The digital forensic laboratory shall use the latest stable versions of its digital forensic tools. Stability decision is subject to the digital forensic laboratory in alignment with the manufacturer announcements. The digital forensic laboratory shall have a manual to cover all the examination domain procedures. Only validated procedures for the intended use shall be used. The digital forensic laboratory shall ensure processing the case image(s) under a virtual case file only. The digital forensic laboratory shall ensure the eradication of the possibility of an acquired image to infect the digital forensic laboratory system directly or indirectly. In addition, the digital forensic laboratory shall ensure that all examiners are trained,

and reminded to escalate the situation, in case of any suspicion of an infection or evidence damage.

4.5.4.2 Examination strategy

The digital forensic laboratory shall ensure building a strategy of digital evidence examination before proceeding with the examination. This strategy shall take into consideration the case evaluation as an input (see 4.5.3.3). The digital forensic laboratory shall ensure that the strategy contains, at least:

a) Examination methodology approach;

b) The required resources to the targeted time frame;

c) Determination of the data capturing approach in accordance with the nature of the case;

d) Appointing the case to a certified digital forensic analyst;

e) Appoint an estimated time frame;

f) The communication matrix of the case;

g) The stakeholder information.

The digital forensic laboratory shall comply with the jurisdiction of digital evidence handling procedures, as it varies from one jurisdiction to another. Unless the evidence is not to be presented to a court, the digital forensic laboratory shall take into consideration in the case strategy the procedures required by jurisdiction (e.g. handling procedures and presentations procedures). The digital forensic laboratory shall take into consideration the investigation strategy, if applicable, during the examination strategy initiation. In addition, it shall have to ensure the suitability of the case strategic approach to the risk stream resulting from case evaluation (see 4.5.3.3). The strategy shall specify a high-level approach of methods to be used, but it should not specify a tool to be used in the examination for instance.

4.5.4.3 Examination preparation

The digital forensic laboratory shall ensure the existence of a documented procedure to prepare evidence to be examined including but is not limited to:

a) Review of the case information, including the case strategy;

b) The use of the digital forensic analyst;

c) Personal protective equipment (e.g. rubber gloves) shall be used

d) The workstation shall be empty, cleaned, and sterilized.

4.5.4.4 Examination: discovery and investigations

The digital forensic laboratory shall have predefined processes of examination, and shall have prescribed procedures of its examination processes including but not limited to the following domains:

a) Test and validation methods;

b) Write protection;

c) Physical and logical imaging;

d) Forensic analysis and data recovery;

e) Mobile device examination;

f) Video analysis;

g) Wiping media.

The prescribed procedures shall be in alignment with the scope of the digital forensic laboratory (see 4.4.1.1.2). The digital forensic laboratory shall have a documented procedure to image digital evidence logically and physically. Physical imaging is capturing all binary data, and the preferred method to be used for data acquisition. Unless it is necessary, the digital forensic laboratory shall only examine the imaged copy of the digital evidence. It shall ensure to document technical notes when a drive is being re-used for another technical service. The digital forensic laboratory shall have a documented procedure to examine mobile devices. The logical acquisition of the examined mobile device, such as data, directory structure, dates and times, shall be accurately reproduced.

The digital forensic laboratory shall ensure the existence of a documented procedure to validate Standard, non-Standard, and internally developed methods. It shall ensure to include methods to be utilized out of its intended scope and modified standard methods prior to being utilized. The examination of digital evidence has to confirm the fitness for purposes and to acknowledge limitations of the method that is intended to be used. The test and validation procedure workflow should be recorded and documented. The digital forensic laboratory shall ensure the existence of a documented procedure and guidance of appropriate practices for processing and the analysis of video recordings. In addition it shall have a known and proved approach in the following areas, at least:

a) Searches;

b) Finding hidden evidence;

c) Extracting files.

The digital forensic laboratory shall ensure the existence of a documented procedure for its covert and remote examinations. The digital forensic laboratory shall ensure the existence of a documented examination and analysis policies, including, at least:

a) Direct data access;

b) The use of evidence copies;

c) Action that may affect the evidence and change the data;

d) The use of original data;

e) Booking, checking, and examine exhibits including but not limited to servers, laptops, personal computers, tablet devices, and cellphones;

f) Acquiring hard disks, tablet computers, and other media;

g) Using devices contain radio transmitters within the digital forensic laboratory faraday shielded area;

h) Data collection;

i) Imaging the evidence, including providing proof of matching the copy with the original exhibit;

j) Hashing and re-hashing the image of the evidence.

The digital forensic laboratory shall ensure the access of the examiners to the technical procedure manual within the work system.

4.5.4.5 Documentation of examination

The digital forensic laboratory shall ensure the existence of a documented process to document the preformed examination. The documents shall be documented either in a common and understandable language or with pre-defined symbols and abbreviated terminologies in a document associated with the documentation. The examination procedures documents shall be available for all examiners. The digital forensic laboratory shall ensure that all processes applied to digital evidence, including the method of acquisition, are detailed and documented and added to the case record and the case file (see 4.5.3.2 and 4.4.2.13). The digital forensic laboratory shall conduct and perform an internal audit on random examination

reports periodically. Documents shall be kept and stored, in the digital forensic laboratory system records (see 4.4.2.13). The evidence examination processes documentation shall be detailed to the level of applying these processes by an auditor or a third party would result in exact same result. The digital forensic laboratory shall ensure that the record has a recorded log, including but not limited to access, preview, and amendment.

4.5.4.6 Reporting a result

The digital forensic laboratory shall ensure the existence of a documented procedure to report its cases internally and externally. The digital forensic laboratory shall not approve the external and final report unless the internal report, is approved by the digital forensic laboratory management. The reports shall be issued with security classification and access (for access control (see 4.5.2.2). The report of the result shall be clear and unambiguously. The internal report shall have, at least, the following:

a) Case information;

b) Used examination methods;

c) Evidence sought;

d) The found evidence;

e) Analysis details;

f) Related appendices.

The digital forensic laboratory shall ensure that all external reports are peer-reviewed, including validation of the findings, and approved by the director. The peer reviewer is fully responsible for what is in the report as much as the original report creator. The digital forensic laboratory shall have a process to validate the report output with the requirements of the case. Also it shall ensure that no case report is released unless it is approved by the director or who has delegated on behalf. The digital forensic laboratory shall ensure to include a declaration in the reports of the cases declaring the status of the knowledge of the laboratory on the acquisition and transportation processes of the evidence at the scene in accordance with accredited International Standards (see 4.5.3.3).

4.5.4.7 Technical manual

The digital forensic laboratory shall ensure the establishment and maintenance of a Technical Manual (TM), which includes but is not limited to:

a) Data recovery and analysis;

b) Write protection;

c) Physical and logical imaging;

d) Test and validation methods;

e) Mobile device examination;

f) Video analysis;

g) Wiping media;

The TM shall be an extension of the QM (see 4.4.2.2.2).

Chapter 5: The Adoption Guideline

5.0 INTRODUCTION

This chapter presents adoption guidance for implementing the draft Standard and its prior and later activities. The chapter articulates the expected challenges to such a journey and draws on experience from previous implementation projects for adopting ISO Standards. Potential success factors for the implementation are identified, and prior activities to the implementation also, such as performing a gap analysis, designing a high-level plan, and creating a business case to evaluate the outcomes. The researcher takes the position that an implementation requires Project Management Methodology (PPM) to manage such a project. The use of a PPM in a functional structural organization, assures consistency and completeness. In addition, the expected outcomes are outlined, and the necessity of establishing an operational project after the implementation for scrutiny of the digital forensic laboratory operation advanced.

5.1 THE OVERALL STRUCTURE OF THE DRAFT STANDARD

To recap the previous chapter, the overall content of the draft Standard is structured into two major classifications: management and technical requirements. The content of the management requirement can be seen in Figure 5.1, where the content of the technical requirement is presented in Figure 5.2. These two figures show further analysis and communication of the design by the researcher.

Figure 5.1: The overall content of the management requirement section of the draft Standard.

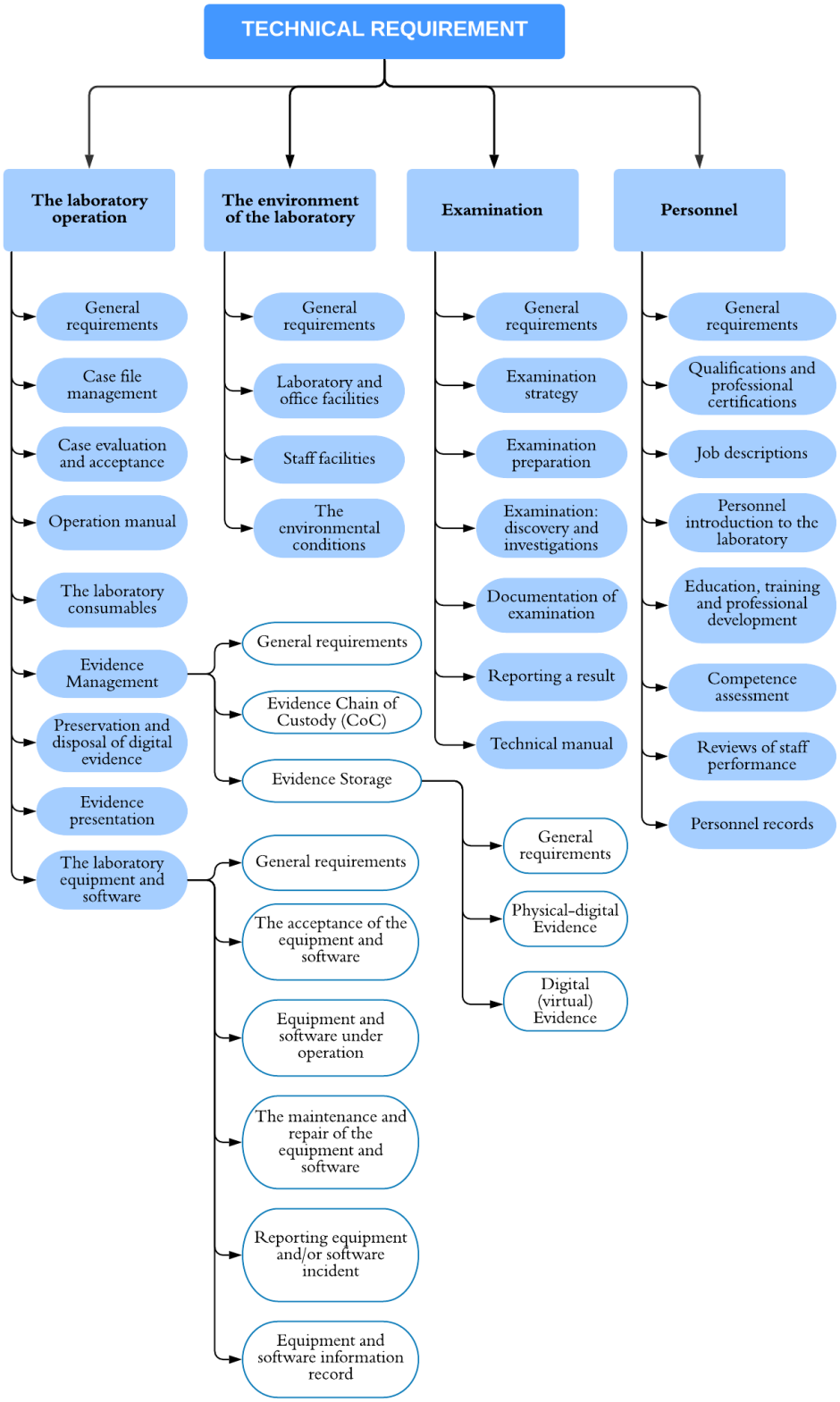


Figure 5.2: The overall content of the technical requirement section of the draft Standard.

Digital forensic laboratories have unique risk due to the nature of digital evidence, but have similarities in the management perspectives with other types of laboratories. In the developed draft Standard there is minor cross over with other International Standards, especially the International Standards for quality. The early analysis (see Chapter 2) showed that other Standards alone are inadequate to cover all digital forensic risks. Similar requirements may not fit perfectly for digital evidence; thus, the author has compared the requirements of the draft Standard with other International Standards for different types of laboratories in Appendix A. It is positioned to treat risk through the improvement of governance mechanisms and the nature of digital evidence.

5.2 IMPLEMENTATION VALUE STREAMS AND CHALLENGES

The ownership of a quality and competence Standards are worth nothing if it is not implemented and maintained effectively. The assurance of the continuity in operation with the expected quality has to be planned from the initial phases of the implementation. The risk of failure in a big change in the organization is high, thus, several key success factors for the stream values are required to ensure the validity of the success factors.

Businesses can be designed on an enterprise level, based on three main domains: governance, management, and core business and supportive dimensions. Together these support the organization's value chain. The core business reflects the core function of the business and focus. The implementation of a quality and competence assurance project may lead to a massive range of changes in the processes, policies, and procedure in the organization. A change range depends on the current situation of the quality level in the organization, which usually extends to affect all levels of the organization’s value chain. The extent of changes result in a culture resistance, which leads to the prevention of productivity. The lack of strong management in this situation would drive the organization to failure and loss of purpose. Such a change during the implementation would cost the organization an enormous amount of money and potential bankruptcy. If law does not require being compliant with a quality Standard, then the conviction of upper management for a return on value would not be strong. This is one of the extensive challenges to the success of the implementation. Managing the implementation project plays a huge role in success,

where if there is no dedicated team, tools, budget and authorisation to manage the implementation, then failure will occur. An organizational change requires project-planning skills, along with delivering the project. The lack of a dedicated team leads to the three dimensions in project management failure: time, scope, and budget. A dedicated project management is required for implementation.

5.3 SUCCESS FACTORS

Six factors support a successful operative implementation. These success factors extend to affect the operation of the digital forensic laboratory after the implementation. In other words, the success of the implementation cannot be measured at the closure point of the implementation project, but the digital forensic laboratory operation has to be evaluated from time to time to avoid deviations. The following sequence of the factors is designed to be in accordance with the timeframe of the adoption journey. Each is itemized as outlined below.

1) Seek full support from the upper management of the digital forensic laboratory.

Having the upper management support the facilitation during the implementation is critical to success. It sends a signal to the whole organization for the willingness to transform the business to be more consistent and quality-focused. The support assists in eliminating conflicts that may result during adoption. This support is mandatory to ensure that such a business transformation is successfully adopted.

2) A clear enterprise architecture plan.

Organizations have the Enterprise Architecture (EA) unit to orchestrate the shape of the organization to fit with the adopted Standard. The capability and knowledge of the EA regarding the business, data, application, and technology of the digital forensic laboratory can play an essential role to assess the current situation of the laboratory and plan a road map to achieve the planned goals. The EA shall play the role of governance during the implementation, to avoid any variation.

3) Always start with a business case.

Organization are advised to start a business case before the implementation, where the idea, the business value, and business cost are analysed. Usually, the business

case identifies the project objective, stakeholders, timeframe, key activities, internal and external resources, dependences, key outputs, key risks and mitigation. Analysing the case shows to the upper management the necessary information to decide on approving the project, which would result in the project to be correctly supported. In addition, the business case can be used in the post-implementation stage to evaluate the overall accuracy of project planning, and this can be used as a lesson learned for future planning for projects.

4) Managing the implementation professionally.

Organizations are advised to assigned dedicated project management professionals to manage the project. It is thought that hiring/assigning a professional Project Manager (PM), and a project management team, may cost the organization an amount of money that they can avoid by assigning that task to one of the personnel in the digital forensic laboratory. A professional from outside can remain focused and only achieve the required objectives. Another advantage of having professional project management is documenting the delivery of the project appropriately, which is professionally required in such an implementation. In alignment with the first success factor, the PM would avoid any disruption to the project stakeholders by creating a communication plan, when is it expected conflicts will occur in such a change to the core business. Organizations that do not have a project management functionality within their structure are advised to assign this task to a third party to ensure having professionals to manage the project.

5) Launch an awareness program.

Resistance can be considered a failure factor, where such a risk can be reduced or even avoided through awareness. The awareness program can be classified based on the audience, where materials shall be designed based on each targeted audience to attract their attention. In other words, executives can be approached with materials revealing the value from such an implementation on an enterprise-level, where managers can be targeted on how such an adoption supports their work to manage the digital forensic laboratory. Similarly, personnel can be targeted revealing how such a change guarantees work quality and how this could impact on them. For instance, if the evidence and its examination is challenged successfully in the court of law the technical changes will have to be made in the laboratory. This awareness program shall be established before the implementation and extend until the closure of the project. After the implementation, the QMS is designed to

govern the work and to make sure all developed procedures are correctly executed.

6) Launch an evaluation project.

The draft Standard is designed to prevent deviation, by establishing preventive and corrective actions. In addition, any deviation is to be discussed in the management review, and organizations are advised to establish an operational project to evaluate the productivity of the implemented quality system. The evaluation can be used to measure the return on investment to the digital forensic laboratory from the cost of implementation to comply with the draft Standard.

5.4 THE ADOPTION JOURNEY

Adopting such a change comes through several stages before implementing the project activities. This section covers what organizations shall perform before establishing the implementation project; and includes assessing the current situation of the digital forensic laboratory, target situation identification, an implementation road map, and the execution of the project.

5.4.1 The Road Map of the Adoption

Organizations start by performing a gap analysis activity to determine the building blocks that are required in order to comply with the competency and quality of the draft Standard. First, organizations are required to assess the digital forensic laboratory current situation to determine the baseline architecture of the organization and the capability to comply with the requirements. After that, the target architecture is the requirements listed in the draft Standard. Then, a gap analysis between the baseline and target architectures has to be performed, and the gap has to be identified, as shown in Figure 5.3. The gap items become the work items that are required to be executed during the implementation. In section (5.1), the EA unit is advised to direct and manage this stage due to their level of knowledge of the enterprise covering the business, data, application, and technology layers across the organization.

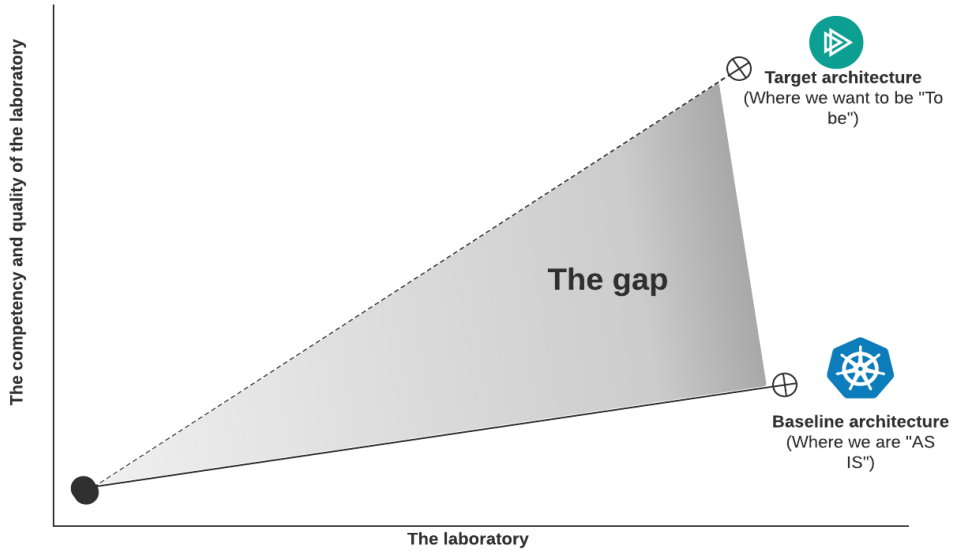


Figure 5.3: The gap analysis. Designed based on the information from *The TOGAF Standard, Version 9.2* (p. 84), by Open Group Standard, 2018: The Open Group.

The goal of the adoption is the strategic direction for the assurance of the quality and competency of the digital forensic laboratory, where the goal of the implementation is focused to carry the organization to reach the target architecture. Thus, the work items that resulted from the gap analysis activity require a high-level plan to be built to implement these items, and this output is considered as the SOW of the project. The work items, within the high-level plan, cannot be cascaded to the level of the project activities at this stage, when this would be broken down during the execution planning process. The work items can be classified to different dimensions, where each aspect can be implemented in parallel within a planned timeline. The project timeline contains milestones, where organizations can evaluate the accomplishments of the implementation and any arisen variations during the project execution. Organizations shall plan to carry out any identified changes arising from the milestones evaluations through a change management process. The overall structure of the high-level plan is shown in Figure 5.4.

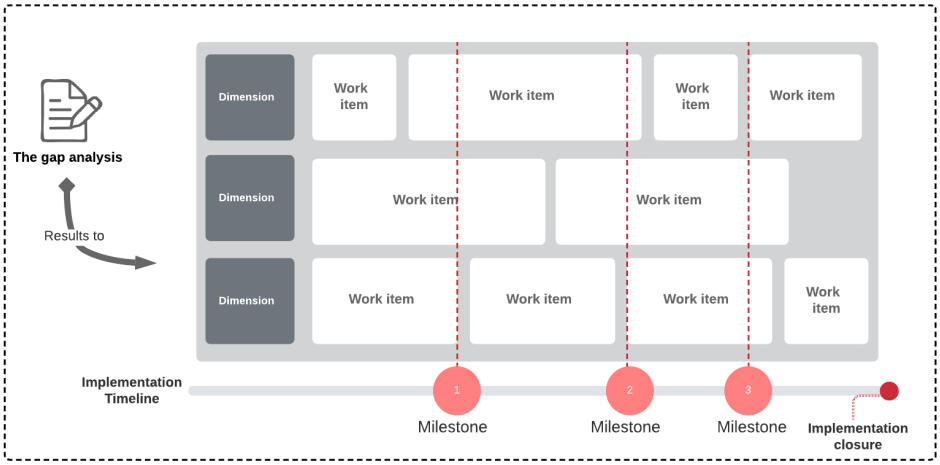


Figure 5.4: The overall structure of the high-level plan.

To approve such a massive project that impacts the whole core business of the digital forensic laboratory, most executives would require a business case to justify the project and to show the return on the investment and the required effort and resources to complete the project. All the above activities are required to build a business case for the adoption. The output of these activities would mostly be used within the project planning process during the planning period within the implementation. The business case is advised to contain, at least, the following:

- **The owner of the project**: An accountable stakeholder for the complete implementation.
- **The objective of the adoption**: Appointing the overall goal for implementing such a draft Standard.
- **Stakeholders**: Identifying internal and external stakeholders, who could be involved in the implementation.
- **Key Activities:** Listed.
- **Timeline**: The start and end dates.
- **Internal sourcing**: Estimating the cost if the organization assuming that the implementation is performed in-house using the full-time personnel of the digital forensic laboratory.
- **External sourcing**: Estimating cost range, while requiring an internal number of full-time employees, assuming the implementation would be outsourced.
- **Key outputs**: Indicating the key tangible and intangible outputs resulting from the completion of the implementation.

- Dependencies: Defining the key prerequisites that should be fulfilled prior to the implementation.

- Key risks and mitigations: Identifying the key risks that could hinder implementation and success.

During the build of the business case, the previous activities that been performed and the outputs, including the gap analysis and the high-level plan, can be used to complete certain sections; for instance, the work items, that resulted from the gap analysis activity, can be used as the key outputs (e.g. documentation, systems, and procedures). A sample of the business case templates are shown in Figure 5.5.

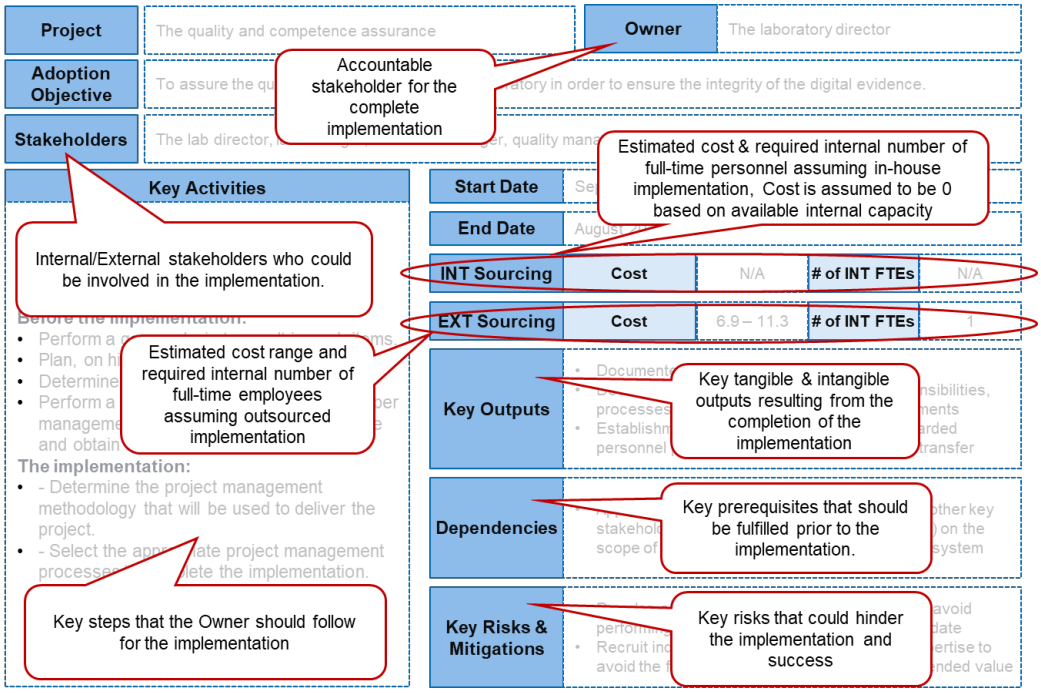


Figure 5.5: Sample of the business case templates. Adopted and *designed based on the information from Tailor the Value-Based Software Quality Achievement Process to Project Business Cases* (p. 56) by Wang, Q., Pfahl, D., Raffo, D. M., Wernick, P., Huang, L., Hu, H., Lü, J., 2006, Germany: © Springer-Verlag Berlin Heidelberg.

As a result of the advised activities, organizations would have a roadmap that defines the digital forensic laboratory directions. In addition, its goals and expected results from the adoption, including high-level steps and milestones required to achieve the plan.

5.4.2 The Implementation Project

Companies invest in massive projects, yet still, projects fail often due to several reasons. One of the reasons is the lack of professional management. Hence, the

implementation of the draft Standard has a high level of risk of failing, which is similar to other strategic projects. It is thought that organizations have the ability to manage their projects since they have the benefit of knowing their business and industry. Unfortunately, managing strategic projects, like other projects, requires certain skills and methodology to manage the project to achieve the targets within the planned time, scope, and budget. To observe the failure rate within a specified industry; for instance, previous studies revealed that over half of IT projects are being cancelled due to inability to deliver the project, where more than 80% are being delivered late due to lack of proper planning and execution (Kraft & Steenkamp, 2010). At the same time, organizations that run under a functional matrix organization structure face a challenge since most of these organizations do not have a PM unit, which is mostly the case with the digital forensic laboratories. The primary obstacle of not having a PM unit within a functional matrix organization structure is that the initiation of a PM unit seems to not be worth the investment since they are operating on functional bases. Thus, the best advice to laboratories is to outsource the management of the project to a third-party. Noting that the laboratory executives have to have clear boundaries between functional managers and the PM.

Notwithstanding the obstacles and challenges that the laboratories may face, the usage of a well-known PPM has its benefits. Adopting a proper PPM is essential to assure the success of the project implementation, which reflects on the success of the organization (Kerzner, 2017). The usage of PPM has several benefits; including but not limited to, documenting the project appropriately, knowledge management, sustainability, success metrics comparability, and iterative improvements (Hanisch, Lindner, Mueller, & Wald, 2009; Hurt & Thomas, 2009; Rosemann, 2015). Therefore, the researcher advises laboratories to adopt a PPM to manage such a strategic change to assure success. One of the well-known methodologies of project management is the methodology of the Project Management Institute (PMI). The PMI has its guidebook called Project Management Body of Knowledge (PMBOK), where it has the knowledge of their approach to managing projects. In September 2017, PMI announced its latest edition of the PMBOK, the sixth edition, and the guidelines state that projects are implemented through several processes; and, these processes are grouped into five groups (Project Management Institue, 2017). These groups can be considered as the

chronological phases of the project, which are: initiating, planning, executing, monitoring and controlling, and closing. In addition, processes have been classified to ten knowledge areas, where each area covers a different dimension. The mapped PMI project management processes based on knowledge areas and process groups are shown in Figure 5.6.

Knowledge Areas	Project Management Process Groups				
	Initiating Process Group	Planning Process Group	Executing Process Group	Monitoring and Controlling Process Group	Closing Process Group
4. Project Integration Management	4.1 Develop Project Charter	4.2 Develop Project Management Plan	4.3 Direct and Manage Project Work 4.4 Manage Project Knowledge	4.5 Monitor and Control Project Work 4.6 Perform Integrated Change Control	4.7 Close Project or Phase
5. Project Scope Management		5.1 Plan Scope Management 5.2 Collect Requirements 5.3 Define Scope 5.4 Create WBS		5.5 Validate Scope 5.6 Control Scope	
6. Project Schedule Management		6.1 Plan Schedule Management 6.2 Define Activities 6.3 Sequence Activities 6.4 Estimate Activity Durations 6.5 Develop Schedule		6.6 Control Schedule	
7. Project Cost Management		7.1 Plan Cost Management 7.2 Estimate Costs 7.3 Determine Budget		7.4 Control Costs	
8. Project Quality Management		8.1 Plan Quality Management	8.2 Manage Quality	8.3 Control Quality	
9. Project Resource Management		9.1 Plan Resource Management 9.2 Estimate Activity Resources	9.3 Acquire Resources 9.4 Develop Team 9.5 Manage Team	9.6 Control Resources	
10. Project Communications Management		10.1 Plan Communications Management	10.2 Manage Communications	10.3 Monitor Communications	
11. Project Risk Management		11.1 Plan Risk Management 11.2 Identify Risks 11.3 Perform Qualitative Risk Analysis 11.4 Perform Quantitative Risk Analysis 11.5 Plan Risk Responses	11.6 Implement Risk Responses	11.7 Monitor Risks	
12. Project Procurement Management		12.1 Plan Procurement Management	12.2 Conduct Procurements	12.3 Control Procurements	
13. Project Stakeholder Management	13.1 Identify Stakeholders	13.2 Plan Stakeholder Engagement	13.3 Manage Stakeholder Engagement	13.4 Monitor Stakeholder Engagement	

Figure 5.6: The mapped PMI project management processes. Reprinted from *Guide to the Project Management Body of Knowledge (PMBOK® Guide)- Sixth Edition* (p. 25), by Project Management Institute, 2017, Pennsylvania, PA: Project Management Institute.

Organizations will adopt the appropriate processes that fit their capabilities. It can be observed that several processes that are shown in Figure 5.6 either have been

performed previously within the sub-section 5.4.1, and it can be utilized as it is; or as a part of the input of the processes. Following is a list and description of the interaction of the performed activities in the PMI processes:

- The organizational processes assets have been identified previously in the baseline architecture in favour of the business requirements, and risks have been appointed within the business case; which can be used within the input to the development of the project charter (process 4.1).
- Stakeholders identification (process 13.1) have been identified within the business case.
- The development of the project plan (process 4.1) has been planned on a high-level, where it is required to be detailed within this process.
- The scope management processes (5.1, 5.2, 5.3, 5.4) have been identified earlier, where the scope is the result of the gap analysis. In addition, the work items that resulted from the gap can be used to build the work breakdown structure (WBS), and the key activities have been identified within the business case.
- The planned timeframe, milestones, and the sequence of the work items that have been mentioned within the high-level plan can be used as an input to the project schedule processes (6.1, 6.2, 6.3, 6.4, 6.5).
- The internal and external cost that have been studied within the business case can be used as an input to the project cost processes (7.1, 7.2, 7.3).
- The risk and mitigation along with the dependencies that have been identified within the business case can be used as an input to the project risk processes (11.1, 11.2, 11.3, 11.5).

Organizations tend to use the PPM to enhance the change to the organization. Although, within this change, the interaction of the role of the PM and functional managers can be extremely challenging to organizations and influence the success of the project. Although the PM is ultimately accountable for the project, the functional managers, project team, and external stakeholders are involved concurrently in several processes within the knowledge areas of the PMI methodology (Kishore, Pretorius, & Chattopadhyay, 2019). In Figure 5.7, the involvement of the PM and others can be seen across the PMI knowledge areas, which illustrate the necessity of the collaboration between parties in the functional organizations, which is the case for digital forensic laboratories. To this end,

organizations are advised to establish clear boundaries between different managerial parties during the implementation. As well as appointing the EA to act as the governance for the project, and to assist in the success of the project.

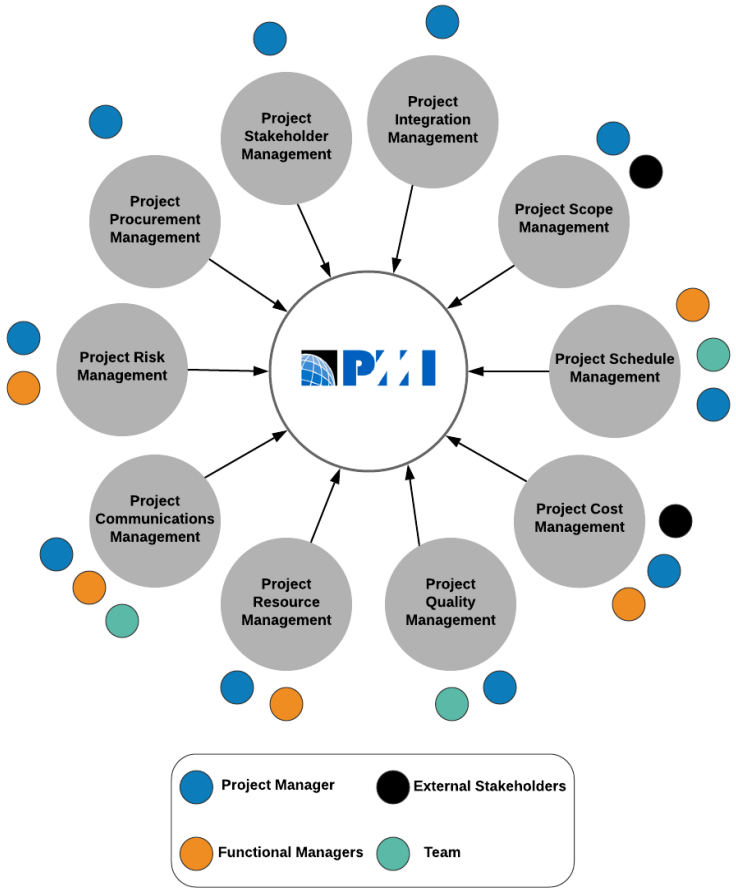


Figure 5.7: The concurrent involvement of the project manager and other parties to the PMI knowledge areas. Redesigned from "The Roles of Functional Managers and Project Managers in a Matrix Organization", by Kishore, N., Pretorius, J. H. C., & Chattopadhyay, G, 2019, IEEE.

While it may be true that the use of the PPM would support the laboratories to implement the draft Standard, there are obstacles. For instance, due to environmental reasons such as interactional between the PM and others. Hence, these obstacles can be eradicated with clear communication, valuable governance, and supportive management.

5.4.3 Continuous Operation

The draft Standard is designed, within its QMS, to record and analyse any potential or existing nonconformities, and appoint a responsible person for following up and

coordinating. After identifying, the cause(s) processes are used until the resolve action(s) is implemented (See 4.3.2.9, 4.3.2.10, 4.3.2.11). The digital forensic laboratory should establish an operational project to periodically evaluate the effectiveness of the entire quality and competency system of the laboratory and improve it. The project shall be carried through the internal audit activities (See 4.3.2.14.5). The result of the evaluation and the improvement suggestions shall be analyzed and applied to the management with a proposed action(s) plan to be discussed and approved through the management review process. In other words, this project can be considered as part of the continuous improvement. (see 4.3.2.12).

5.4.4 The Overall Adoption Journey

To summarize the overall adoption journey, the journey can be divided into three main stages: prior to the implementation, the implementation project, and the continuous improvement. The first stage contains assessing the current situation and gathering the requirements along with studying the required effort to perform the changes during the implementation. The second stage is the implementation project by the adoption of the PMI methodology. The second stage is divided into two: the delivery of the project and the governance of the project. The third stage is post-implementation, where an iteration project is advised to be launched to monitor and improve the quality and competency system of the digital forensic laboratory. These three stages and the interaction with the functional units and areas of the organization are shown in Figure 5.8.

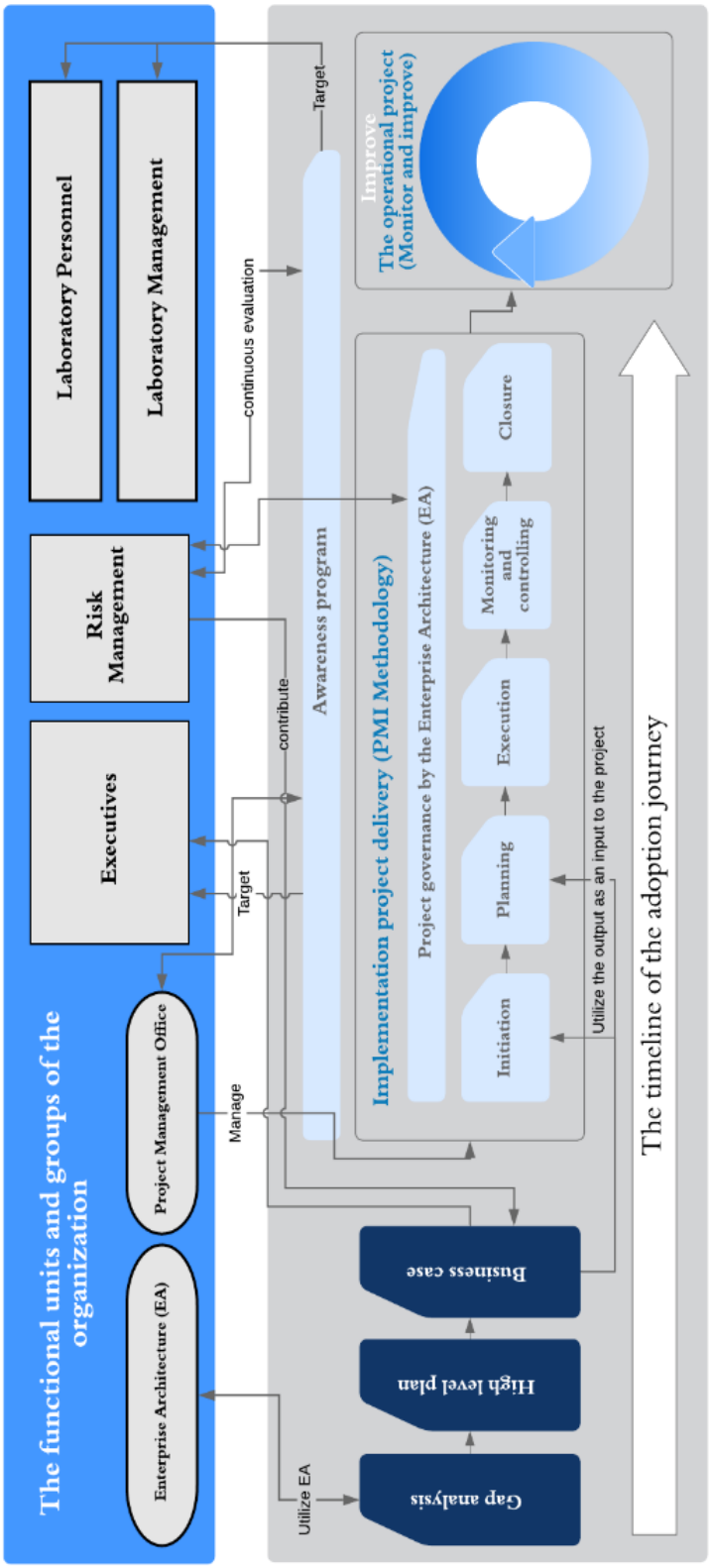


Figure 5.8: The overall journey of the adoption of the draft Standard.

5.5 THE EXPECTED RESULT

Standards guide organizations on what the requirements to be met, but not how to achieved them. Organizations have different methods to fulfil those requirements, but in general, certain outputs can be expected. Generally, the implementation outputs can be categorized within the EA four layers: business, information, application, and technology, as shown in Figure 5.9. The digital forensic laboratory target architecture from the implementation is an update to current architecture, which is a prior assessment before the implementation.

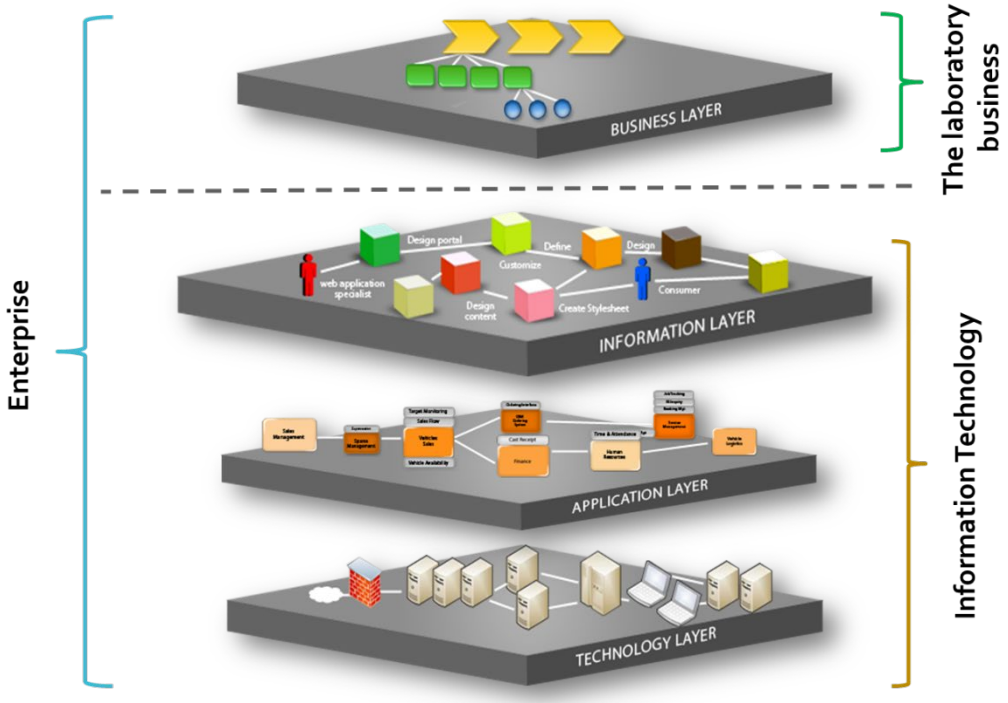


Figure 5.9: The Enterprise Architecture layers. Designed based on the information from *The TOGAF Standard, Version 9.2* (p. 77-130), by Open Group Standard, 2018: The Open Group.

The detailed result of the implementation of the draft Standard in accordance to the EA business layer, illustrates the necessity of transforming the laboratory business to be guided by quality management documentation, and the manuals. The overall laboratory manuals shall have its structure and hierarchy, as shown in Figure 5.10, where the QM shall be the highest authority level for laboratory operations. In addition, it presents the other expected manuals that includes Technical, Operations, Training, and Health and Safety.

Figure 5.10: The Organizational policies of the quality management

The above graphic illustrates the relationship of the laboratory system of quality management documentation and the draft Standard, along with the government regulations and law. As defined earlier, in 4.4 and 4.5, the Standard is categorised into two major components: Management and Technical. The QM maps directly to the draft Standard and states how the digital forensic laboratory meets the draft Standard requirements. Where policies and procedures are sufficiently defined in the QM, they will stand as the sole authority. However, there are documents which require a greater level of detail to describe the step-by-step procedures that the digital forensic laboratory employees must perform to complete a process. This level of detail is in the appropriate subordinate operations manual, which refers to the day-to-day operations. The TM, presents the approved technical procedures. The TRM defines the digital forensic laboratory training program and professional

development of personnel that map to the technical services. In addition, the foundation for evidence of conformance to the draft Standard and the digital forensic laboratory requirements can be referred to in the records produced and stored in the document management system. Compliance with the draft Standard requires the support of IT. The implementation of the draft Standard would mostly lead to the digital forensic laboratory to implement new software or to adjust a current one, or to install new equipment. These IT elements should be considered as an output of the implementation of the draft Standard. These outputs can be categorised in accordance with the information, application, and technology layers of the EA. In summary, all the resulting elements from the implementation within the IT domains are expected to impact and update the EA layers.

5.6 CONCLUSION

The adoption journey of a Standard has challenges that are managed by planning. Organizations shall assess their current situation to analyse the gap and to create a target architecture. A high-level plan supports the business case in order to measure the expected effort. The findings of this chapter indicated that there are serval success factors that organizations should follow to ensure a successful implementation and better value gains.

In the management of the project, this chapter articulated that even with the utilize of a PPM, the project may still face challenges since the digital forensic laboratories mostly operate on a functional-basis, and not as a project driven organization. It is thought that prior activities to the implementation may lead to wasted effort, however, it was explained how all the prior activities could fit into the detailed planning when the implementation began. To this end, the implementation has its expected outputs on the business level, such as QM, OM, TM, TRM, and health and safety manual. The draft Standard is designed to ensure continuous improvements and avoid glitches by the performance of corrective and preventive actions. Organisations shall establish an operational project after the implementation to evaluate the effectiveness of the entire quality and competency system of the digital forensic laboratory through the internal audit activities. In the following Chapter 6 the expert feedback on the draft Standard is reported.

Chapter 6: The Validation (Expert feedback)

6.0 INTRODUCTION

This chapter presents the validation phase of the draft Standard by consulting four experts to provide feedback to improve the draft Standard. The chapter begins by first articulating the credentials of the experts, and then reports the feedback and analyses. This chapter can be considered as a pathway to the following chapter, where recommendations are being made for future research.

6.1 EXPERT FEEDBACK

To verify the artefact, the researcher has consulted several experts seeking their feedback and comments on the draft Standard. The draft Standard was provided to the experts to comment on the content and provide feedback on it from their years of field experience. The feedback was received over the period from January 7, 2020, to February 5, 2020. The method that has been used to obtain the feedback is that the experts were provided with the draft Standard, and requested to provide their feedback, comments, and answer several questions, which are presented in 3.3.2. These evaluate the artefact and provide their comments on any gap or deficiency of the draft Standard. According to clause 6.7 of the Auckland University of Technology Ethics Committee (AUTEC) regulation (see in Appendix C), this type of activity is ethically pre-approved.

The experts are working at a large-scale organization handling different types of forensic cases such as digital, bioterrorism, epidemiology, toxicology, anthropology, biology, and DNA analysis; but the digital forensic laboratory that each expert operates is an entirely independent unit from the others. The first expert, who hereinafter is referred to as ‘Expert 1’, has more than twenty years of experience within the forensic domains. Expert 1 has an education background in computer engineering, forensic science, and criminal psychology. Expert 1 work experience background is across forgery, terrorism, and digital evidence. Expert 1 is a digital forensic laboratory director for over than ten years.

The second expert, who hereinafter is referred to as ‘Expert 2’, has more than

ten years of experience. Expert 2 has an education background in the Information and Communication Technology (ICT) domains and cybercrime. Expert 2 has more than ten years of experience in examining digital evidence, and he/she is the digital forensic laboratory manager. His/her experience involves building strategies for the digital forensic laboratory case management.

The third expert, who hereinafter is referred to as 'Expert 3', has more than ten years of experience. Expert 3 has an education background within the Engineering Technology areas. Expert 3 is responsible for the quality of the digital forensic laboratory, as the quality manager, for the past four of years. In addition, expert 3 has significant experience in managing the logistic services of the digital forensic laboratory.

The fourth expert, which hereinafter is referred to as 'Expert 4', has more than ten years of experience examining digital evidence. Expert 4 has an education background in computer science and data engineering. Expert 4 professionally accredited with more than ten professional certifications.

6.2 THE RECEIVED FEEDBACK

The received feedback from the consulted experts, as part of the research methodology, is listed as follows:

Expert 1 suggests that the digital forensic laboratory should have an expertise system, where there is a classification of examiners based on multiple criteria such as years of experience, the domains of experience, education background, and training background. The system would allow the digital forensic laboratory to appoint and address the cases correctly. In addition, the cross-validation of examinations can be addressed with such a system to avoid uncertainties in the procedures. Expert 1 doubts that small scale laboratories or laboratories with a tight budget can comply with such a large number of requirements due to the high cost of complying to the draft Standard. Expert 1 urges the researcher to have different levels of the requirements in each domain, where the foundation level presents the basic requirements that the digital forensic laboratory is required to comply with; and the quality of the laboratory can be upgraded to the next level with more strict requirements. This is similar to the Standardized methodology tier 1,2,3, and 4 for the data centres where at each level the availability guarantees

percentage increases, expert 1 says.

Expert 1 stated that the digital forensic laboratory would receive every now and then digital evidence covered with biological evidence such as fingerprints, blood, and hair. This type of evidence often has high priority due to the involvement within a crime or terrorist act for instance. Thus, the expert believes that the digital forensic laboratory shall be able to examine biological evidence within its SOW, at least the most common one. Expert 1 indicates that the rapid growth and change in technology has led the digital forensic laboratory to launch projects to acquire different types of knowledge and thus it has different affects, directly and indirectly, on the performance quality. The draft Standard did not cover this gap. Thus, the expert suggested having the existence of a research centre within the digital forensic laboratory as a requirement. This centre can be utilized to transfer the knowledge across the technical team, expert 1 says. In addition, it would be exceptionally good if the centre launches periodic sessions to transfer the experience between the digital forensic laboratory examiners.

Expert 2 indicates that even though the Standard presented the requirement to perform an examination by referral digital forensic laboratories and/or consultants, in subsection 4.5.2.5.1, but occasionally laboratories may require to utilize a third-party service in a different stage than the examinations. For instance, to examine the evidence on arrival to ensure the status of the evidence in exceptional cases such as digital evidence effected by a nuclear attack. Another example, but much simpler, is when laboratories are required to utilize a third-party service in a different science in the partial support to analyse the evidence during the examination; for instance, in terrorist cases, examiners often require translator support to translate documents and messages written in a foreign language. The expert articulates that other than case referral to other digital forensic laboratories, the draft Standard did not cover this gap in contracting the digital forensic laboratory with a third party, individual or organization, to support in different stages within a different specialties.

Expert 2 says that the draft Standard did not cover initial biological examination of digital evidence, which has been exposed to a nuclear or epidermal environment for instance. This activity is to verify the safety of examining it digitally without affecting the health of the examiner(s). Expert 2 suggests having an Evidence Manager (EM), where he/she will be accountable for the evidence unless the evidence is handled to the examiner for examination. The EM is the one

responsible for the governance of the CoC to guarantee the accuracy of the record. In addition, the EM should be able to access the temporary evidence storage, where only the EM and the examiner have access to the temporary storage containers.

Expert 3 comments that the draft Standard guarantees the existence of a procedure to ensure that there are no conflicts of interest in the acceptance of the evidence. However, given the nature of the digital evidence, a conflict of interest might arise during the analysis of the data, which the draft should ensure the existence of a procedure for the examiner to stop the examination and report the situation to his/her superior. Expert 3 notes that the digital forensic laboratory may be forced to interact with different government entities, where these entities may have procedures that affect the integrity of the evidence, and the digital forensic laboratory may face a situation where the case cannot be rejected. Another example the expert referred to that in different countries the government forces the courier companies to observe the delivered item as part of the service acceptance; in this situation, the integrity of the digital evidence, may be violated. Thus, the digital forensic laboratory should have a procedure to declare in the case report for a disclaimer for the digital forensic laboratory in guaranteeing the integrity of the evidence in these circumstances. Expert 3 also observes that the draft Standard is missing regulating working remotely as part of the competency of the digital forensic laboratory.

Expert 4 indicates that the draft Standard specifies, in 4.5.4.4, the requirement of ensuring the access of its technical procedure manual within the workstation. Often the procedure is dependent upon the use of a particular type of hardware or software and mostly vendor manuals have sufficient detailing of the procedures within its manual. Thus, it would be more convenient when the digital forensic laboratory has to ensure the existence of a copy of all the vendor's user manuals in each workstation, to have at least one copy electronically available. Expert 4 also indicates that the forensic video analysis is being articulated as a requirement within the examination procedures requirements, but the audio analysis is not mentioned. The expert agrees that video analysis may cover to a certain degree the audio analysis, but there are sectionalized tools to handle audio forensic, which are required to have documented procedures.

Expert 4 points out that the draft Standard address that the physical-digital evidence shall be recorded in the storage inventory management system (see

4.5.3.6.3.2), where this system manages all types of items such as consumables. In addition, under the evidence management, it is mentioned in the draft Standard that examined evidence shall be documented and tracked through the DFS (see 4.5.3.6.1). Similarly, under the case file management, it is articulated that all the technical records shall be recorded and stored securely in the DFS (see 4.5.3.2). The expert argues that handling physical-digital evidence in multiple systems would be a waste of effort and it may result in human errors during the data entry. This would require a huge amount of effort in auditing the records. Thus, it is advised to use the DFS as a default system to document, record, track, and manage the physical-digital evidence, where the evidence is required to be logged in the inventory system through a scanning code, only to retain records to manage the storage smoothly.

6.3 ANALYSIS OF THE FINDINGS

The consulted experts are named experts based on their level of experience in a certain domain, but some of their feedback may require further investigation and confirmation with other digital forensic experts in cross-validation. Thus, the researcher filtered the recovered feedback based on the current knowledge, where feedback acknowledged and accepted as an improvement to the draft Standard. On the other hand, feedback, which is acknowledged, but requires future research to investigate the validity, is addressed for future work. The feedback, which is believed to require further research to be clarified, is held in extra notes for future work. The overall summary of the expert feedback can be seen in Figure 6.1.

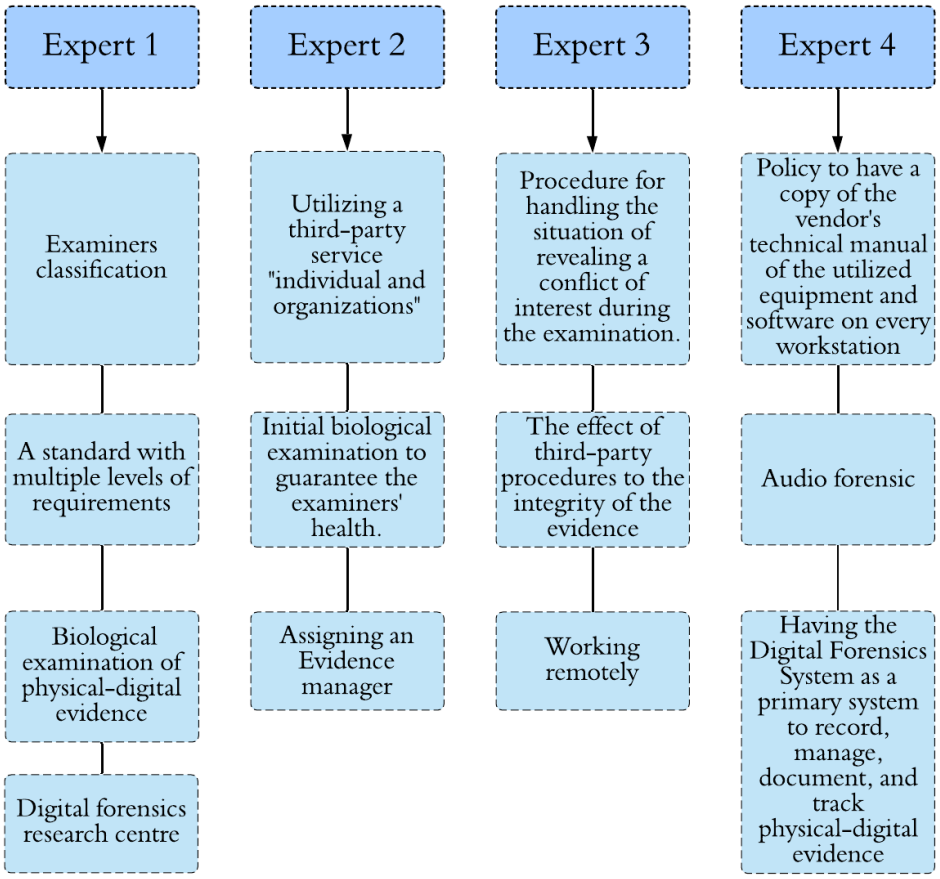


Figure 6.1: An overall summary of expert feedback

Figure 6.2 illustrates the overall of the expert 1 feedback, and it can be analysed as followed:

The expert 1 feedback regarding the research centre could contribute to the rapid growth of technology, which would improve the design quality and competence system. The researcher notes that the scope of the research centre could be expanded to cover the control of the authorized methods of examination. Also, the centre could lead the digital forensic laboratory on the improvement of its processes, for instance, investigating the delay of the cases lifecycle to observe any gaps, and changes to the digital forensic laboratory processes; through the digital forensic laboratory management review process.

The expert 1 feedback regarding the biological examination can be aligned with the expert 2 feedback regarding the initial biological check to guarantee the health of the examiners. This process can be considered as an essential process for all evidence arriving after the acceptance of the case. On the other hand, the digital

forensic laboratory shall ensure documented procedures to handle evidence that has been exposed to any biological damage to protect the digital forensic laboratory environment. In addition, the initial biological examination space shall be isolated from the digital laboratory rooms to avoid any contamination.

The expert 1 feedback regarding the classification of the examiners can be considered for launching a transfer of knowledge programme through the research centre, where senior examiners should be used to support junior examiners to increase the level of their knowledge.

The expert 1 feedback regarding having multiple levels of the requirements and the IT data centre tier levels may not be feasible. The researcher argues that the IT data centre tier levels can be measured by the availability percentage of the services, in contrast, the integrity of the evidence can be violated easily, and the designed quality system shall ensure that there are no breaches during the processes. Thus, the researcher believes that the nature of the digital forensic laboratories has its differences with others, such as IT data centres. However, it could be possible, thus, the feedback requires further research.

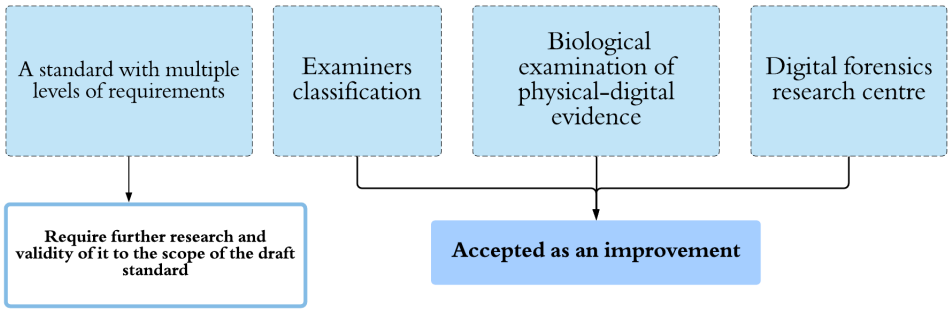


Figure 6.2: The overall summary of expert 1 feedback

Figure 6.3 illustrates the overall contribution of the expert 2 feedback, and it can be analysed as follows:

The expert 2 feedback regards assigning an EM to be accountable for handling the evidence process. It seems that assigning an owner to the process of handling the evidence would appoint an accountable agent for the evidence in each case. The purpose of designing a process is to ensure the consistency of workflow, which is handling the evidence in such a situation. An extra requirement of having a dedicated manager for evidence would increase the cost of compliance to the draft Standard, where such a step would require further research and cross-validation to justify the need for more details.

The expert 2 feedback regarding the initial biological examination has been acknowledged and merged with the expert 1 feedback regarding the biological examination of the physical-digital evidence.

The expert 2 feedback regarding utilizing third-party services. This would be an amendment to the subsection (4.4.2.4); where the digital forensic laboratory shall ensure to have its service agreement for third-party services. The laboratories shall ensure having a non-disclosure agreement to be signed by the service provider. In addition to that, the digital forensic laboratory shall ensure to include utilizing a third-party if required, under its SLA with the customer. On the other hand, subsection 4.4.2.5.1 would require an amendment to expand the scope of the referral examinations to cover the entire laboratory activities.

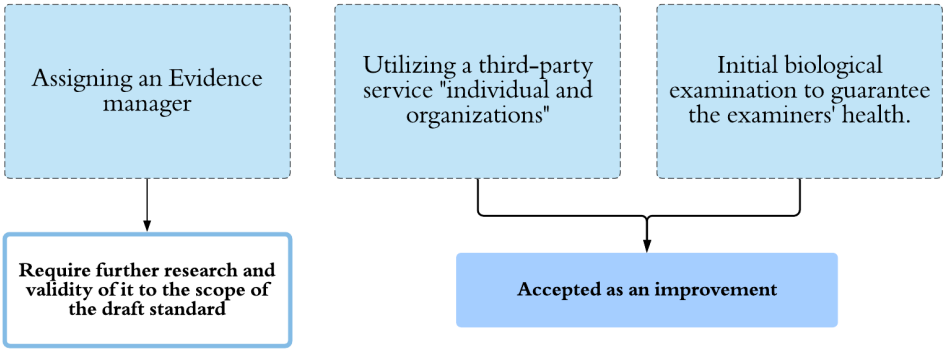


Figure 6.3: The overall summary of expert 2 feedback

Figure 6.4 illustrates the overall of the expert 3 feedback, and it can be analysed as follows:

The expert 3 feedback regards working remotely. The draft Standard is designed to ensure the continuity of the digital forensic laboratory business even remotely under the sub-section (4.4.2.16). The business continuity should be designed, to be activated in the case of a disaster, not in a normal situation. Thus, this would require further research to investigate wither it is safe to allow examiners to work remotely. In addition, this feedback articulates a new gap for investigating the quality and competency of working remotely from a technical perspective as part of the BCM.

The expert 3 feedback regarding having a procedure for handling the situation of revealing a conflict of interest during the examination is included in the draft Standard that is designed to address any potential conflicts of interests before the examination. The feedback can be addressed as an amendment to the ethical

conduct in the sub-section (4.4.1.1.3); where a note has to be added:

NOTE: The digital forensic laboratory shall have a documented procedure to handle any arising conflicts of interests that may be reveal during the examination.

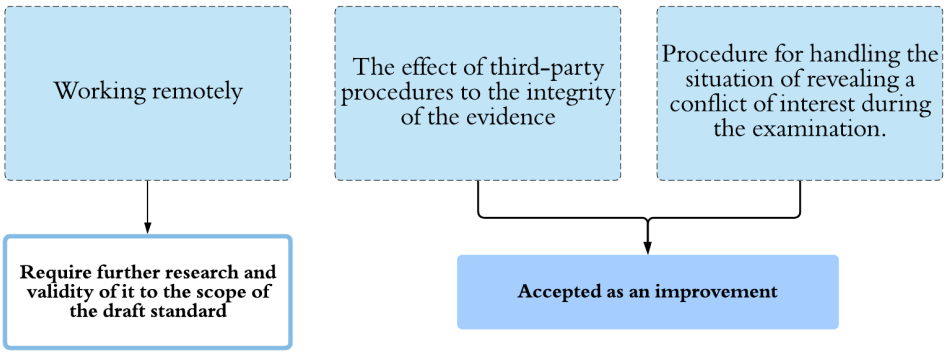


Figure 6.4: The overall summary of expert 3 feedback

Figure 6.5 illustrates a summary of the expert 4 feedback, and it can be analysed as follows:

The expert 4 feedback regarding the audio forensic can be addressed with the video analysis as an amendment to the subsection (4.5.4.4). To be: The digital forensic laboratory shall ensure the existence of a documented procedure and guidance of appropriate practices for processing and analysis of video and audio recordings.

Regarding the expert 4 feedback on adding a copy of the vendor TM of the utilized equipment and software on every workstation, the Standards usually advise organizations on the requirements to be met and not how to meet these requirements. Thus, it can be addressed as an amendment to (4.5.4.4) as a note: The digital forensic laboratory shall ensure the access of the examiners to the technical procedures manual, including the vendor user manuals, within the workstation. In addition, the digital forensic laboratory has the choice either to add it as part of the digital forensic laboratory TM or to add the vendors' manuals as a separated document.

Lastly, regarding the expert 4 feedback on having a primary system to record, manage, document, and track physical-digital evidence; this could be an amendment to: Subsection (4.5.3.3): The digital forensic laboratory shall ensure the following condition: Evidence is entered, numbered, and labelled in the DFS, and logged into the inventory management system when the evidence is entered into storage. In this case, the evidence would be handled through the DFS, but it would

be required to be logged or scanned during the attempt to enter the evidence into the storage. This step would be only for the purpose of managing the storage easily. In addition, laboratories could integrate the inventory management system into the DFS to update the status and location of the evidence automatically.

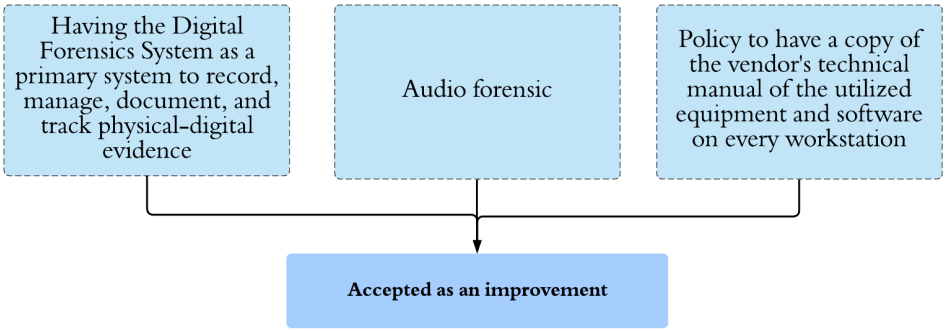


Figure 6.5: The overall summary of expert 4 feedback

6.4 CONCLUSION

In this chapter, the last step of the research methodology was covered through the consultation of four experts within the digital forensic domain. The feedback was conducted over the course of a month in early 2020. The findings showed thirteen matters of feedback to improve the draft Standard. The feedback was reviewed and studied carefully to see how to fit it into the draft Standard. Some of the feedback appears to require further research. Others have been acknowledged, and accepted as improvement items to the Standard. The analysis of the findings presents gaps that may require further research from a technical perspective. A significant finding is the establishment of a research centre within the digital forensic laboratory aiming to improve the operation of the digital forensic laboratory. The gaps and other suggestions are presented as recommendations for future research in the following chapter.

Chapter 7: The Recommendations and Conclusion of the Research

7.0 RECOMMENDATIONS FOR FUTURE RESEARCH

For digital forensic laboratories to comply with the requirements of the draft Standard would result in organizational changes, and change management cost. Consequently, executives tend to avoid these costs unless they have to. The researcher believes that there are two scenarios to encourage the laboratories to invest in such a change. First, when the compliance is mandatory by law, so that no evidence is accepted in the court of law if the examined evidence has been performed in a laboratory, which has not, complied. Second, when the lawyers are encouraged to challenge the examined digital evidence and its integrity, verification of due and compliant practices are required. Thus, the lack of current motivation to certify Digital Forensic Laboratories against digital forensic Standards requires scrutiny. The entire digital forensic ecosystem requires motivation to invest in standarised, workable, certifiable and quality practices. The ecosystem approach should be implemented in two dimensions: domestic and International.

Furthermore, the researcher faced challenges to determine the level of coverage of the requirements. Should all digital forensic sub-domains have more details? Would this make the draft Standard too costly and unworkable? For instance, the quality controls for the digital forensic laboratory operating remotely are far greater than the current proposal. New research could cover the design of a Standard in multiple versions, where each version spans a certain domain or level. For instance, there can be versions for the quality of the technical perspective and another version can be a guide to the governance of the digital forensic laboratory.

The technology challenges for digital forensic laboratories, requires accommodation of the rapid growth of technology capability. Cloud solutions are not always permissible. Laboratories are forced to invest in equipment, software, hardware, change processes and procedures. Therefore, continuous changes would require a QMS designed to improve its dynamics as part of its processes. The management of technology impacts digital evidence and affects the entire

laboratory operation. For example, today examination must be performed in the secure laboratory, but one-day laboratories may have to operate in the cloud, which would change the entire operating model including the quality and competency processes and procedures. Sudden changes in the operation have to be considered. For example, the coronavirus pandemic, known as COVID-19, that took a place in early 2020, forced changes in business models where everyone had to operate through the internet. If a similar instance occurs in the future for a longer period, digital forensic laboratories would have to change and use virtualized forensic processes. Thus, future research is advised to take into consideration the flexibility in changing the digital forensic laboratory operation. In this research, the experts' feedback is to establish a research centre within the digital forensic laboratory with the main purpose of continuous enhancement of the technical dimension of its operation. This is an indication of the importance of adapting to the future challenges by research aimed to design a responsive system.

The digital forensic laboratories have a consistent operating model from one country to another. Hence, further research is required into customizing laboratories to local laws and cultural expectations. This is to include multiple scopes, where an evaluation from one entity or one country is not enough to cover all requirements. For instance, there are multiple types of laboratories such as government laboratories, military laboratories, and privately owned laboratories. The requirements for each type of these laboratories would be different, thus, future research is advised to verify the requirements with different experts from different countries, and different types of laboratories.

Furthermore, one of the challenges that requires further research is the reduction of the negative impact of the constant changing of legislation on the laboratories. It is widely known that digital transformation has reached the level of maturity; with the support of rapid growth in could computing, to transform the core of businesses. This would result in an increase in the number of cybercrimes worldwide, where this is expected to result in the increase of the number of cases that are required to be handled by digital forensic laboratories. For that problem, researchers are encouraged to investigate methods on speeding up the lifecycle of cases, and to achieve the targeted speed with the guarantee of the quality in the result. These recommendations are made to improvement the digital forensic ecosystem and to impact, directly and indirectly, positively on the quality of the

evidence examination delivered by digital forensic laboratories.

7.1 CONCLUSION

The rapid growth in technology has led to an increase in crimes committed using technological solutions or the presence of these solutions in the crime scenes. However, the possibility of the contamination or manipulation of digital evidence is high due to the nature of digital evidence. The digital evidence can be examined and analysed using specialised equipment and software within a digital forensic laboratory but processes have to be standardised to assure the worth of the evidence. Digital forensic laboratories must aim to control the quality and competency of the digital forensic laboratory through the adoption of an International Standard. With the absence of a digital forensic Standard, there is a problem. With no specified Standard researchers have published statements advocating for such since the year 2000. They have referred to in the literature, the absence of a specified digital forensics laboratory Standard, and yet after a decade, the absence remains the same.

The ISO/IEC 17025, has been taken as a general Standard for the competence of testing and calibration laboratories, but applied to specific levels of risk associated with digital evidence inappropriately. The ISO/IEC 17025 has been adapted to accredit a digital forensics laboratory without adjusting the Standard to fit the requirements, and leaving elements of risk (points of failure) out of scope. The establishment of a new digital forensic laboratory Standard requires a strenuous of effort to motivate and to mobalise the digital forensic community into action. The DS research methodology has through a sequence of activities, been used to identify the problem and design a solution to the problem. The draft Standard has been developed, and expert feedback received to motivate action from a clearly defined starting point.

The research has presented a proposal for a draft International Standard for Digital Forensic Laboratories and an implementation guideline. The guideline gives a structure to analyse the gap in a current digital forensic laboratory position, against a target architecture that is supported by the Standardization document. A well-known PPM has been advised to be adopted, to implement the resulted scope of work. Later, the launch of an operational project has been advocated to periodically evaluate the implemented system and improve it.

This research has made two significant contributions to knowledge. First, the theoretical framework for the standardisation of forensic laboratories has been evaluated and found incomplete in the coverage of scope. Second, the specific example of the Digital Forensic Laboratory guidance for practice has been written. In the first instance, this research elaborates and innovates thinking for making the theory more complete, and by methodology demonstrates how to perform better and more inclusive theory. In the second instance, the artefact and its improvement in two cycles give a result that can be taken to the next stage in practice. The expert feedback was crucial in establishing the relevancy of the artefact and also to improve the fit with practice. The implementation guide is also a contribution to knowledge and relevant to practitioners. Finally, the artefact can be moved into the ISO workgroup that standardises digital forensics as an input for discussion and the basis for a new work item.

Furthermore, several recommendations have been made for future research, where the improvement of the digital forensic ecosystem would impact, directly and indirectly, on the quality of the evidence examination within digital forensic laboratory.

References

Competency or management system based standards? Frequently asked questions. (2016). Retrieved from https://www.iso.org/files/live/sites/isoorg/files/archive/pdf/en/casco-faq.pdf

Date, D. (2013). ISO/IEC JTC 1/SC 27 Information technology-Security techniques Secretariat: DIN, Germany.

Eekels, J., & Roozenburg, N. F. (1991). A methodological comparison of the structures of scientific research and engineering design: their similarities and differences. *Design studies, 12*(4), 197-203.

Fal', O. M. (2017). Standardization in Information Technology Security. *Cybernetics and Systems Analysis, 53*(1), 78-82. https://doi.org/10.1007/s10559-017-9908-8

Gómez-Ochoa, N. G., Ortega-Chasi, P., Alvarado-Cando, O., Cobos-Cali, M., & Artega-Sarmiento, S. (2020). Eye Tracking in the Diagnosis of Aggressive Behaviors and Emotions: A Systematic Review of the Literature [10.1007/978-3-030-20476-1_13]. In T. Ahram, (pp. 111-121). Cham: Springer International Publishing.

Grobler, M. (2012). The Need for Digital Evidence Standardisation. *International Journal of Digital Crime and Forensics (IJDCF), 4*(2), 1-12.

Guo, H., & Hou, J. (2018). Review of the accreditation of digital forensics in China. *Forensic sciences research, 3*(3), 194-201.

Hallstrîm, K. T. (2004). *Organizing international standardization: ISO and the IASC in quest of authority*: Edward Elgar Publishing.

Hanisch, B., Lindner, F., Mueller, A., & Wald, A. (2009). Knowledge management in project environments. *Journal of Knowledge Management, 13*(4), 148-160. https://doi.org/10.1108/13673270910971897

Hatto, P. (2013). Standards and standardisation: A practical guide for researchers. *Luxembourg: European Commission, Publications Office of the European Union*.

Hevner, A., & Chatterjee, S. (2010). *Design research in information systems: theory and practice* (Vol. 22): Springer Science & Business Media.

Hibbard, E. (2014). Electronic discovery standardization. *Ave Maria L. Rev., 12*, 313.

Hurt, M., & Thomas, J. L. (2009). Building value through sustainable project management offices. *Project Management Journal, 40*(1), 55.

Hykš, O., & Koliš, K. (2014). Development of the Digital Forensic Laboratory Management System Using ISO 9001 and ISO/IEC 17025. *IDIMT–Interdisciplinary Information Management Talks. Linz: Trauner Verlag*, 87-94.

International Laboratory Accreditation Cooperation (ILAC). (2015). *The ILAC Mutual Recognition Arrangement*. Retrieved from https://ilac.org/?ddownload=891

International Organization for Standardization. *The facts about certification*. Retrieved August 27, 2019, from https://www.iso.org/certification.html

International Organization for Standardization. *What is CASCO?* Retrieved August 27, 2019, from https://www.iso.org/casco.html

International Organization for Standardization. (2008). *Quality management systems - Requirements* (ISO 9001:2008). Geneva: International Organization for Standardization.

International Organization for Standardization. (2014). *The ISO Survey of Management System Standard Certifications*. Geneva, Switzerland. Retrieved from https://www.iso.org/files/live/sites/isoorg/files/archive/pdf/en/iso_survey_executive-summary.pdf

International Organization for Standardization. (2015a). *Incident investigation principles and processes* (ISO/IEC 27043:2015). Geneva: International Organization for Standardization.

International Organization for Standardization. (2015b). *Storage security* (ISO/IEC 27040:2015). Geneva: International Organization for Standardization.

International Organization for Standardization. (2017). General requirements for the competence of testing and calibration laboratories (ISO/IEC 17025:2017).

ISO - Technical Committes Retrieved 24 Aug, 2019, from https://www.iso.org/technical-committees.html

Judges on E-Discovery: Keep It in Perspective. (2013). *Information Management Journal, 47*(4), 7-7.

Kao, D.-Y., Chao, Y.-T., Tsai, F., & Huang, C.-Y. (2018). Digital Evidence Analytics Applied in Cybercrime Investigations*IEEE.* Symposium conducted at the meeting of the 2018 IEEE Conference on Application, Information and Network Security (AINS)

Kerzner, H. (2017). *Project management : case studies* (Fifth edition. ed.) [Electronic document]: Wiley. Retrieved from https://search.ebscohost.com/login.aspx?direct=true&db=cat05020a&AN=aut.b19979939&site=eds-live

http://ebookcentral.proquest.com/lib/AUT/detail.action?docID=4841877

Kim, B. S., Kim, Y. D., Hwang, C. K., & Yoo, J. H. (Eds.). (2007). A mechanism of KEDB-centric fault management to optimize the realization of ITIL based ITSM [Conference Paper]. *4773 LNCS*, 72-81. Retrieved from https://www.scopus.com/inward/record.uri?eid=2-s2.0-38149066025&partnerID=40&md5=d4d35f2ed23154938250a4b952f48ca7

Kishore, N., Pretorius, J. H. C., & Chattopadhyay, G. (2019). The Roles of Functional Managers and Project Managers in a Matrix Organization (pp. 784-788): IEEE.

Klipper, S. (2011). Information Security Risk Management. *Risikomanagement mit ISO/IEC, 27001*, 27005.

Kraft, T. A., & Steenkamp, A. L. (2010). A Holistic Approach for Understanding Project Management. *International Journal of Information Technologies & the Systems Approach, 3*(2), 17.

Liberati, A., Altman, D., Tetzlaff, J., Mulrow, C., Gøtzsche, P., Ioannidis, J., . . . Moher, D. (2009). The PRISMA statement for reporting systematic reviews and meta-analyses of studies that evaluate healthcare interventions. *Bmj, 339*.

Long, J. (2008). *ITIL Version 3 at a Glance : Information Quick Reference* [Book]. [New York]: Springer. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=edsebk&AN=248

041&site=eds-live
Marshall, A. M., & Paige, R. (2018). Requirements in digital forensics method definition: Observations from a UK study (Vol. 27, pp. 23-29).
Moher, D., Liberati, A., Tetzlaff, J., & Altman, D. G. (2009). Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement. *Annals of internal medicine, 151*(4), 264-269.
Murphy, C. N., & Yates, J. (2009). *The International Organization for Standardization (ISO): global governance through voluntary consensus*: Routledge.
Nunamaker Jr, J. F., Chen, M., & Purdin, T. D. (1990). Systems development in information systems research. *Journal of management information systems, 7*(3), 89-106.
Oxford Dictionary of English, 3 ed. (2010). In A. Stevenson (Ed.), [Book
English Dictionary]. https://doi.org/10.1093/acref/9780199571123.001.0001
Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of management information systems, 24*(3), 45-77.
Project Management Institue. (2017). *A Guide to the Project Management Body of Knowledge (PMBOK® Guide)*. Newtown Square, PA, United States: Project Management Institute,. Retrieved from http://ebookcentral.proquest.com/lib/aut/detail.action?docID=5180849
Rao, L., Mansingh, G., & Osei-Bryson, K.-M. (2014). *Knowledge Management for Development : Domains, Strategies and Technologies for Developing Countries* [Book]. New York: Springer. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=edsebk&AN=696483&site=eds-live
Riillo, C. A. (2013). Profiles and motivations of standardization players. *International Journal of IT Standards and Standardization Research (IJITSR), 11*(2), 17-33.
Rosemann, M. (2015). The Service Portfolio of a BPM Center of Excellence. *Handbook on Business Process Management 2: Strategic Alignment, Governance, People & Culture*, 381.
Scientific Working Group on Digital Evidence. (2018). *SWGDE Establishing Confidence in Digital and Multimedia Evidence Forensic Results by Error Mitigation Analysis*.
Seo, D. (2013). Analysis of various structures of standards setting organizations (SSOs) that impact tension among members. *International Journal of IT Standards and Standardization Research (IJITSR), 11*(2), 46-60.
Sommer, P. (2018). Accrediting digital forensics: What are the choices? (Vol. 25, pp. 116-120).
Sonntag, M. (2013). Evidence collection for critical infrastructure. *IDIMT-2013: Information Technology Human Values, Innovation and Economy*, 23-30.
Takeda, H., Veerkamp, P., & Yoshikawa, H. (1990). Modeling design process. *AI magazine, 11*(4), 37-37.
Tantra, R. (2016). *Nanomaterial Characterization: An Introduction*: John Wiley & Sons.
Tao, K.-m., Li, X.-q., Zhou, Q.-h., Moher, D., Ling, C.-q., & Yu, W.-f. (2011). From QUOROM to PRISMA: a survey of high-impact medical journals' instructions to authors and a review of systematic reviews in anesthesia literature. *Plos One, 6*(11), e27611-e27611.

https://doi.org/10.1371/journal.pone.0027611
Veber, J., & Klíma, T. (2014). Influence of Standards ISO 27000 Family on Digital Evidence Analysis. *Proceedings of the 22nd Interdisciplinary Information Management Talks*, 103-114.
Walls, J. G., Widmeyer, G. R., & El Sawy, O. A. (1992). Building an information system design theory for vigilant EIS. *Information systems research, 3*(1), 36-59.
Wang, Q., Pfahl, D., Raffo, D. M., Wernick, P., Huang, L., Hu, H., . . . Lü, J. (2006). Tailor the Value-Based Software Quality Achievement Process to Project Business Cases. In (pp. 56). Retrieved from https://search.ebscohost.com/login.aspx?direct=true&db=edb&AN=32893305&site=eds-live
Watson, D., & Jones, A. (2019). *Digital forensics processing and procedures : meeting the requirements of ISO 17020, ISO 17025, ISO 27001 and best practice requirements* [Electronic document]: Syngress. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=cat05020a&AN=aut.b13163164&site=eds-live
http://ezproxy.aut.ac.nz/login?url=http://ebookcentral.proquest.com/lib/aut/detail.action?docID=1115161
Wieringa, R. J. (2014). *Design science methodology for information systems and software engineering*: Springer.
Wilson-Wilde, L. (2018). The international development of forensic science standards — A review. *Forensic Science International, 288*, 1-9. https://doi.org/10.1016/j.forsciint.2018.04.009

Appendix A: THE OVERLAP OF THE DRAFT STANDARD WITH OTHER INTERNATIONAL STANDARDS

The building of Standardization requirements in a specific field overlaps other International Standards, for example in this proposal presented here, the ISO17025 and ISO 15189. The below table compares the requirements of the draft Standard with other International Standards. Requirements tagged with symbols indicate that the requirements, which cross with other Standards, have different conditions and these conditions comes as follow:

- The stared (*) requirements have been improved in the draft Standard to fit the nature of digital evidence.

- The hashed (#) requirements have been improved in the draft Standard with more governance requirements.

- The requirements in the draft Standard that tagged with a dollar symbol ($) are mandatory, where in other Standards they are an option.

- The requirements in the draft Standard that tagged with a percentage symbol (%) mitigate outstanding digital evidence completely, where others cover it partially.

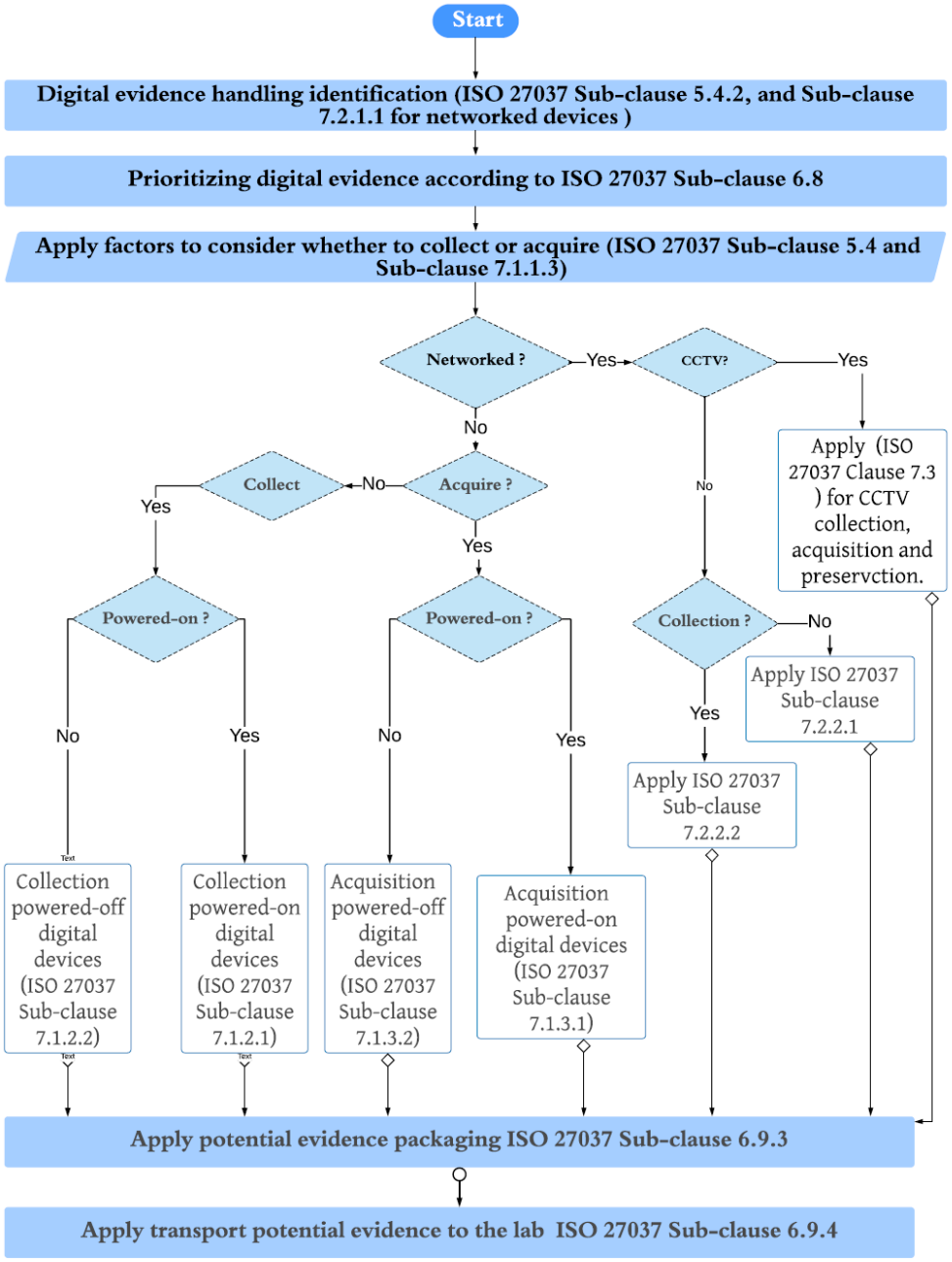
Requirement	The draft Standard "ISO 270XX"	ISO 17025	ISO 15189
Organisation	4.3.1.1	4.1, 4,2, 5.1, 5.2, 5.4, 5.5	4.1
Management responsibility (#)	4.3.1.2	4.1.2, 5.7	4.1.2
Tasks responsibilities, accountabilities, interrelationships and communication (#)	4.3.1.2.5, 4.3.1.2.6	5.5	

Documentation requirements (#, %)	4.3.2.2	8.1, 8.2 (Optional)	4.2.2
Document control	4.3.2.3	7.11	4.3
Service agreements	4.3.2.4	7.1,	4.4
Examination by referral digital forensic laboratories	4.3.2.5	6.6.1, 6.6.2, 6.6.3	4.5
External services and supplies	4.3.2.6	6.6	4.6
Advisory services	4.3.2.7	N/A	4.7
Resolution of complaints	4.3.2.8	7.9	4.8
Identification and control of nonconformities	4.3.2.9	7.4.2, 7.10	4.9
Corrective and preventive actions ($, #)	4.3.2.10, 4.3.2.11	8.7 (Optional)	4.10, 4.11
Continuous improvement (#)	4.3.2.12	8.6	4.12
Control of records	4.3.2.13	7.10.2, 8.1.2 (Optional)	4.13
Evaluation and audits	4.3.2.14	8.8	4.14
Management review (#)	4.3.2.15	8.9 (Optional)	4.15
Business Continuity Management	4.3.2.16	N/A	N/A
Personnel	4.4.1	6.2	5.1
The digital forensic laboratory environmental conditions	4.4.2	6.3	5.2
Evidence Chain of Custody	4.4.3.6.2	N/A	N/A
The digital forensic laboratory equipment, software, and consumables (*)	4.4.3.4, 4.4.3.5	6.4	5.3.1, 5.3.2
Case evaluation and acceptance	4.4.3.3	N/A	N/A
Evidence Management	4.4.3.6	N/A	N/A
Evidence Storage (Physical-digital Evidence and Digital “virtual” Evidence)	4.4.3.6.3.1, 4.4.3.6.3.2, 4.4.3.6.3.3	N/A	N/A
Preservation and disposal of digital evidence (*)	4.4.3.7	7.4.1, 7.4.4 (doesn’t fit	N/A

		digital evidence)	
Evidence presentation	4.4.3.8	N/A	N/A
Examination strategy (#, *)	4.4.4.2	7.2	N/A
Examination preparation	4.4.4.3	N/A	N/A
Digital evidence Examination processes (*)	4.4.4.4	7.7 (doesn't fit digital evidence)	N/A
Documentation of examination (*)	4.4.4.5	7.7.1	5.5.3
Reporting a result (*)	4.4.4.6	7.5.1, 7.5.2, 7.8	N/A

Appendix B: EVIDENCE HANDLING PROCESSES PRIOR TO LABORATORY ARRIVAL

Laboratories are advised to require the evidence processes to comply with the below flow chart.



Appendix C: ETHICS EXCEPTIOIN

EXCEPTIONS TO ACTIVITIES REQUIRING AUTEC APPROVAL

The following activities do not require AUTEC approval:

6.7. Where a professional or expert opinion is sought, except where this is part of a study of the profession or area of expertise.

-See more detail at: https://www.aut.ac.nz/research/researchethics/guidelines-and-procedures#6