Chapter 3

Setting up the Forensic Laboratory

Table of Contents

3.1 SETTING UP THE FORENSIC LABORATORY

This chapter is the summary of many small elements, each of which gives guidance on areas that will need to be considered from the planning stage onward. All of the elements discussed below will need to be addressed both for good management and for preparation for accreditation and certification for the Forensic Laboratory.

When initially setting up the Forensic Laboratory, there are a number of issues that will need to be considered. Many of these have been touched on in the previous chapters, and some are expanded here, others have dedicated chapters later in the book. Once the business case (or the equivalent if in government or law enforcement) has been developed, a range of issues will need to be addressed and these must be documented to describe the fundamental basis on which the Forensic Laboratory is being established and on which it

will be run. The first issue that should be clearly documented is that of the Forensic Laboratory's Terms of Reference (ToR). There will also normally be a ToR for the project to develop and deliver to the Forensic Laboratory, but the concepts that are given below hold good for both cases.

3.1.1 Forensic Laboratory Terms of Reference

The ToR is the document that serves as the basis of the relationship between the owning organization of the Forensic Laboratory and the team responsible for carrying out the work. It describes the purpose and structure of the Forensic Laboratory and shows how the scope of the Forensic Laboratory will be defined and verified. It will also provide the yardstick against which the success of the Forensic Laboratory will be measured. It provides a documented basis for future decisions and for a common understanding of the scope among the stakeholders.

The ToR sets out a clear path for the operation of the Forensic Laboratory by stating what needs to be achieved, by whom and when. It identifies the set of deliverables that satisfy the requirements and the scope and any constraints should be set out in this document. The ToR for the operation of the Forensic Laboratory should be created during the earliest stages of the project for the establishment of the Forensic Laboratory immediately after the business case has been approved. Once the ToR has been approved, there is a clear definition of the scope of the Forensic Laboratory.

The ToR will also identify the success factors, risks, and boundaries. The ToR needs to be written in some detail and should include the following:

- vision;
- scope and objectives;
- deliverables;
- boundaries, risks, and limitations;
- roles, responsibilities, authority, accountability, and reporting requirements;
- stakeholders;
- the regulatory framework;
- resources available;
- work breakdown structure and schedule;
- success factors;
- intervention strategies.

A description of the ToR is given in Appendix 1.

Once the ToR has been developed, a range of other elements that outline how the Forensic Laboratory is structured and how it will operate need to be developed.

3.1.2 The Status of the Forensic Laboratory

There should be clear statement of the status of the Forensics Laboratory. This should define the ownership, the services that it will offer, the structure of the laboratory, the standards that it will work to, and the expected customers. This should be prepared in some detail as it will be the foundation for future decisions.

3.1.3 The Forensic Laboratory Principles

The Forensic Laboratory shall be run in accordance with the following laboratory principles:

3.1.3.1 Responsibilities

The Forensic Laboratory relies upon the Laboratory Manager to develop and maintain an efficient, high-quality forensic laboratory.

The Laboratory Manager holds a unique role in the balance of scientific principles, requirements of the Criminal Justice System, and the effects on the lives of individuals that may be subject of an investigation that relies on digital forensic evidence. The decisions and judgments that are made in the Forensic Laboratory must fairly represent all interests with which they have been entrusted.

Users of the Forensic Laboratory services must be able to rely on the reputation of the Forensic Laboratory, the abilities of their Forensic Analysts, and the standards of the profession.

3.1.3.2 Integrity

The Forensic Team must be honest and truthful with their peers, supervisors, and subordinates. They must also be trustworthy and honest when representing the Forensic Laboratory to outside organizations.

3.1.3.3 Quality

The Forensic Team is responsible for implementing quality assurance procedures which effectively monitor and verify the quality of the work product of their laboratories.

The Forensic Laboratory complies with the requirements of ISO 9001 and ISO 17025.

3.1.3.4 Efficiency

The Forensic Team should ensure that the Forensic Laboratory's products and services are provided in a manner which maximizes organizational efficiency and ensures an economical expenditure of resources and personnel.

3.1.3.5 Productivity

The Laboratory Manager should establish reasonable goals for the production of forensic casework in a timely fashion. Highest priority should be given to cases which have a potentially productive outcome and which could, if successfully concluded, have an effective impact on the enforcement or adjudication process.

3.1.3.6 Meet Organizational Expectations

The Laboratory Manager must implement and enforce the relevant organizational policies and procedures and should establish additional internal procedures designed to meet the ever-changing needs of forensic case processing.

3.1.3.7 Health and Safety

The Laboratory Manager shall be responsible for planning and maintaining systems that reasonably assure safety in the Laboratory as well as when the Forensics Team are in the field. Such systems should include mechanisms for input by the Forensic Team, maintenance of records of injuries, and routine safety inspections as defined by existing Health and Safety procedures.

The Forensic Laboratory complies with the requirements of OHSAS 18001.

3.1.3.8 Information Security

The Laboratory Manager shall be responsible for planning and maintaining the security of the Forensic Laboratory. Security measures should include control of access both during and after normal business hours.

The Forensic Laboratory complies with the requirements of ISO 27001.

3.1.3.9 Management Information Systems

The Laboratory Manager shall be responsible for developing management information systems. These systems should provide information in a timely manner regarding current and past work carried out by the Forensic Laboratory.

3.1.3.10 Qualifications

The Laboratory Manager must hire employees of sufficient academic qualifications or experience to provide them with the fundamental scientific principles for work in the Forensic Laboratory and must be assured that they are honest, forthright, and ethical in their personal and professional life.

3.1.3.11 Training

The Laboratory Manager shall provide training in the principles and the details of forensic science as it applies to the Forensic Laboratory requirements.

Training must include handling and preserving the integrity of physical evidence. Before analysis and casework are performed, specific training for the processes and procedures as well as for the specific tools to be utilized must be undertaken. A full training program for all Forensic Analysts and Investigators must be developed.

3.1.3.12 Maintaining Employee Competency

The Laboratory Manager must monitor the skills and proficiency of the Forensic Analysts on a continuing basis as well as on an annual basis as required by Human Resources procedures. The Forensic Laboratory has an ongoing program of training, awareness, and competency.

3.1.3.13 Employee Development

The Laboratory Manager must foster the development of the Forensic Analysts and Investigators for greater job responsibility by supporting internal and external training, providing sufficient library resources to permit the Forensic Analysts and Investigators to keep abreast of changing and emerging trends in forensic science, and encouraging them to do so. The Forensic Laboratory has an ongoing program of training, awareness, and competency.

3.1.3.14 Environment

The Laboratory Manager must ensure that a safe and functional work environment is provided with adequate space to support all the work activities required by the Forensic Laboratory. Facilities must be adequate so that evidence under the control of the Forensic Laboratory is protected from contamination, tampering, or theft.

3.1.3.15 Supervision

The Laboratory Manager must provide the Forensic Analysts and Investigators with adequate supervisory review to ensure the quality of their work product. The Laboratory Manager must be held accountable for the performance of the Forensic Analysts and Investigators and the enforcement of clear and enforceable processes and procedures.

The Forensic Analysts and Investigators should be held to realistic performance goals which take into account reasonable workload standards.

The Laboratory Manager must ensure that the Forensic Analysts and Investigators are not unduly pressured to perform substandard work through case load pressure or unnecessary outside influence. The Forensic Laboratory shall have in place a performance evaluation process.

3.1.3.16 Conflicts of Interest

The Laboratory Manager, the Forensic Analysts, and the Investigators must avoid any activity, interest, or association that interferes or appears to interfere with their independent exercise of professional judgment.

The Forensic Laboratory Conflict of Interest Policy is given in Appendix 3.

3.1.3.17 Legal Compliance

The Laboratory Manager shall establish and publish, with appropriate training, operational procedures in order to meet good procedural, legislative, and good practice requirements.

3.1.3.18 Accountability

The Laboratory Manager and the Lead Forensic Analyst must be accountable for their decisions and actions.

These decisions and actions should be supported by appropriate documentation and be open to legitimate scrutiny.

3.1.3.19 Disclosure and Discovery

The Forensic Laboratory records must be open for reasonable access when legitimate requests are made by Officers of the Court or other legitimate requesters.

Specific requirements are necessary for the release of unlawful material.

3.1.3.20 Work Quality

The Laboratory Manager must establish a quality assurance program.

The Forensic Analysts and Investigators must accept responsibility for evidence integrity and security; validated, reliable methods; and casework documentation and reporting.

The Forensic Laboratory complies with the requirements of ISO 9001 and ISO 17025.

3.1.3.21 Accreditation and Certification

The Laboratory Manager shall achieve and maintain whichever certifications and accreditation that the Top Management deem necessary.

3.1.3.22 Membership of Appropriate Organizations

The Laboratory Manager shall ensure that the Forensic Team joins appropriate professional organizations and that they are encouraged to obtain the highest professional membership grade possible.

3.1.3.23 Obtain Appropriate Personal Certifications

The Laboratory Manager shall ensure that the Forensic Team achieves appropriate certifications of both generic and tool-specific types to demonstrate their skill levels.

3.1.4 Laboratory Service Level Agreements

A Service Level Agreement (SLA) is a part of a service contract where the level of service that will be provided by the digital forensics laboratory is formally defined. The SLA is sometimes used to refer to the contracted delivery time for the services offered by the Forensic Laboratory (usually called the "Turn Round Time") or the quality of the work. The SLA should be considered from the start of the planning and development process to ensure that the Forensic Laboratory will be structured to the appropriate level. Service providers normally include SLAs within the terms of their contracts with customers to define the level of service that is being provided in plain language using easily understood terms. Any metrics included in a SLA must be measurable and should be tested on a regular basis. The SLA will also normally outline the remedial action and any penalties that will take effect if the delivered service falls below the defined standard. The SLA forms an essential element of the legal contract between the Forensic Laboratory and the customer. The actual structure of the SLA will be dependent on the services offered by the Forensic Laboratory, but the general structure of the agreement is as follows:

- contract;
- amendments;
- service description;
- service availability;
- reliability;
- customer support;
- service performance;
- change management procedures;
- security;
- service reviews;
- glossary;
- amendment sheet.

If the Forensic Laboratory takes services from either an external supplier (e.g., Internet Access or utility supplier) or from the owning organization (e.g., human resources or logistics), then suitable SLAs will need to be agreed with the service provider.

3.1.5 Impartiality and Independence

In order to obtain and retain accreditation to ISO 17025 (general requirements for the competence of testing and calibration laboratories), there is a requirement for the Forensic Laboratory to be able to show evidence that its work and results are "free from undue influence or pressure from customers or other interested parties" and that "laboratories working within larger organizations where influence could be applied (such as police laboratories), are free from such influence and are producing objective and valid results."[a]

3.1.6 Codes of Practice and Conduct

In the United Kingdom, the Forensic Regulator has produced Codes of Practice and Conduct for forensic science

a. UK House of Commons, Publications on Science and Technology, http://www.publications.parliament.uk/pa/cm201012/cmselect/cmsctech/855/85506.htm#n129.

providers and practitioners in the Criminal Justice System. These Codes of Practice and Conduct were the first stage in the development of a single quality standards framework for forensic science for use in the Criminal Justice System to replace the *ad hoc* approach to standards that had been used in the past. These Codes of Practice and Conduct were built on the internationally recognized good practice of ISO 17025 as the preferred standard for forensic science laboratories.

An appendix to these Codes of Practice and Conduct provides guidance to deal with the specific requirements for the providers of forensic science services at scenes of incidents based on ISO 17020 (general criteria for the operation of various types of bodies performing inspection). This standard for inspection bodies is gradually being adopted across Europe as the most appropriate standard for crime scene investigations.

The requirements that are described in the Codes of Practice and Conduct and the associated appendices are targeted at three levels:

- the organization: to outline what is required of it, particularly from the management, with regard to quality assurance and compliance. Most forensic services are supplied by people working in organizations and the organizational culture with regard to quality is a major factor. Accountability for quality rests with the management, and each organization is required to nominate a senior manager as the "accountable person";
- the practitioner: to outline the professional standards to which they are expected to perform; and
- the scientific methodology: to ensure that the methodology is robust and will reliably produce, and continue to produce, valid results.

These Codes of Practice and Conduct were developed so that they can be applied to all organizations and practitioners whose primary role is the provision of forensic services into the Criminal Justice System in England and Wales. While these Codes of Practice and Conduct were designed for the UK community, they are based on sound principles and international standards, are a good guideline and a basis for codes of practice for other regions, and have been adopted by the Forensic Laboratory.

3.1.7 Quality Standards

Quality standards in forensic science are essential to ensure that the highest possible standards are maintained by the Forensic Laboratory as a supplier of forensic services. This should include resourcing, training, equipment, processes, and integrity benchmarks such as accreditation. Unless these standards are maintained, there is an increased possibility that those guilty of crimes may not be brought to justice or that those who are innocent may be convicted. Quality standards in forensic science are best attained through accreditation to the international standard ISO 17025, which builds on the older ISO 9001 standard. However, on its own, ISO 17025 will not guarantee quality, as it does not cover areas like setting of the Forensic Laboratory strategy for a case, or the interpretation of the results, or the presentation of the evidence in the Court. A cross reference between ISO 9001 and ISO 17025 is given in Appendix 2. This clearly shows a close correlation, but ISO 17025 has more technical competences in it than ISO 9001.

3.1.8 Objectivity

A professional Forensic Analyst or Investigator, when providing any service, must determine whether there are any threats to compliance with the fundamental principle of objectivity. These threats will normally result from the Forensic Analyst, Investigator (or the Forensic Laboratory itself) having interests in, or a relationship with any member of the Client organization. An example of a familiarity threat to objectivity could be created from a family or close personal or business relationship. Independence of thought is necessary to enable the professional Analyst or Investigator to express a conclusion, without bias, conflict of interest, or undue influence from others.

The existence of threats to objectivity when providing any professional service will depend upon the specific circumstances of the engagement and the nature of the work. A professional Forensic Analyst or Investigator must evaluate the significance of any threats and, when necessary, ensure that suitable measures are taken to eliminate threats or reduce them to an acceptable level. Examples of the types of measures that may be considered include the following:

- advising the management of the Forensic Laboratory of the potential threat;
- the Forensic Analyst or Investigator removing themselves from the case;
- the Forensic Laboratory having in place suitable peer review and supervisory procedures;
- terminating the relationship that gives rise to the threat.

If the measures that have been put in place to eliminate or reduce threats to an acceptable level are not effective, the Forensic Laboratory management must either decline or terminate the contract with the customer. The Forensic Laboratory Conflict of Interest Policy is given in Appendix 3.

3.1.9 Management Requirements

There are many ways in which management requirements can be expressed. The Forensic Laboratory has implemented an Integrated Management System (IMS) based on the Publicly Available Specification 99 (PAS 99). Full details of the IMS are given in Chapter 4.

This has allowed the Forensic Laboratory to implement the following ISO standards:

- ISO 15489—Information and documentation—Records management;
- ISO 17020—Conformity assessment—Requirements for the operation of various types of bodies performing inspection;
- ISO 17025—General requirements for the competence of testing and calibration laboratories;
- ISO 22301—Societal security—Business continuity management systems;
- ISO 27001—Information technology—Security techniques—Information security management systems—Requirements;
- ISO 9001—Quality management systems—Requirements;
- OHSAS 18001—Occupational Health and Safety Management Systems;
- In-house digital forensic procedures.

3.1.10 Forensic Laboratory Policies

In order to assure the integrity of their results, the Forensic Laboratory must have appropriate policies in place. The implementation of these policies will be in the form of practices and procedures that define how the Forensic Laboratory will operate to meet the relevant good practice and forensic science and quality standards. The constant developments in technology mean that there is an ongoing need to update the policies in order to meet changing laws and regulations in order to prevent unfairness and wrongful conviction. The Forensic Laboratory policies must ensure the integrity of any results produced.

The main purpose of policies within the Forensic Laboratory is to assure the integrity of results and to prevent miscarriages of justice. There are many examples of mistakes within laboratories. One example is the analysis of the data in the Casey Anthony trial in July 2011, when the number of times that she had accessed the internet to search for the word "Chloroform" was initially reported as 84 times but was later found to be only one time.[b,c] Another example is the CD Universe case where the evidence was compromised because the chain of custody was not properly established.[d] Policies are also necessary to ensure that the employees within the Forensic Laboratory receive and are able to maintain a suitable level of training and certification, and they should also address funding levels and the policy on investigation of allegations of misconduct or negligence. The policies should also contain sections on the code of ethics and the relevant standards and regulations.

3.1.11 Documentation Requirements

The relevant standards implemented within the Forensic Laboratory will dictate much of the required documentation for everyday operations. Documented procedures are included in the relevant chapters in this book.

3.1.12 Competence, Awareness, and Training

All management standards have requirements for competence, awareness, and training. All Forensic Laboratory employees must also be aware of client requirements and the relevance of their activities. They should understand how their actions contribute to achieving the Forensic Laboratory's Quality Policy and objectives. This is normally achieved by awareness training, performance reviews, and employee participation in internal audit processes. Top Management should define the necessary skills, experience, and training required for each role and identify the records of education, training, skills, and experience that need to be maintained. The Forensic Laboratory Quality Policy is given in Appendix 4.

3.1.13 Planning

There are a number of actions that need to be taken throughout the planning process. These include the following:

3.1.13.1 Risk Assessment and Management

A fundamental element of the planning process is the Risk Assessment. The objective of the Risk Assessment is to discover and document the current risks and threats to the business and to identify and implement measures to mitigate or reduce the risks that carry the highest probability of occurring or the highest impact. This Risk Assessment document should give guidance on how to conduct the Risk Assessment and also how to evaluate and analyze the information that is collected. It should also contain guidance for the organization on how to implement strategies to manage the potential risks.

Risk Management in the Forensic Laboratory is covered in Chapter 5.

3.1.13.2 Business Impact Analysis

The Risk Assessment is only one part of an overall Business Assessment. The Business Assessment is divided into

b. Forensic Data Recovery, Digital Evidence Discrepancies—Casey Anthony Trial, July 11, 2011, http://wordpress.bladeforensics.com/?p=357.

c. The State v. Casey Anthony: Analysis of Evidence from the Case, July 18, 2011, http://statevcasey.wordpress.com/tag/digital-forensics/.

d. CD Universe evidence compromised, http://www.zdnet.com/news/cd-universe-evidence-compromised/96132.

two parts, the Risk Assessment and a Business Impact Analysis (BIA). The Risk Assessment is intended to measure the present risks and vulnerabilities to the business's environment, while the BIA evaluates the probable losses that could occur as a result of an incident. To maximize the value of a Risk Assessment, a BIA should also be completed. A BIA is an essential element of an organization's business continuity plan. The BIA should include an assessment of any vulnerabilities and plans for the development of strategies to minimize risk. The BIA describes the potential risks to the organization studied and should identify the interdependencies between the different parts of the organization and which are the critical elements. For example, the Forensic Laboratory may be able to continue to operate more or less normally if the plumbing system failed but would not be able to function if the network failed.

As part of a business continuity plan, the BIA should identify the probable costs associated with failures, such as loss of cash flow, cost of facility repair, cost of equipment replacement, overtime payments to address the backlog of work, loss of profits, etc. A BIA report should quantify the importance of the individual elements of the Forensic Laboratory and suggest appropriate levels of funding for measures to protect them. Potential failures should be assessed in terms of the financial cost and the impact on legal compliance, quality assurance, and safety. Business Continuity is covered in Chapter 13.

3.1.13.3 Legal and Regulatory Considerations

The investigation of crimes involving digital media and the examination of that digital media in most countries are covered by both national and international legislation. In criminal investigations, national laws normally restrict how much information can be seized and under what circumstances it can be seized. For example, in the United Kingdom, the seizure of evidence by law enforcement officers is governed by the Police and Criminal Evidence Act (1984) and the Regulation of Investigatory Powers Act (2000) (RIPA). The Computer Misuse Act (1990) provides legislation regarding unauthorized access to computer material, and this can affect the Investigator as well as the criminal and is a particular concern for civil investigators who have more limitations on what they are allowed to do than law enforcement officers.

In the United States, one of the pieces of legislation that the investigator must be aware of is the rights of the individual under the Fourth Amendment, which limits the ability of government agents to search for and seize evidence without a warrant. The Fourth Amendment states:

"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

According to OLE,[e] the Supreme Court stated that a "seizure of property occurs when there is some meaningful interference with an individual's possessory interests in that property," *United States v. Jacobsen*, 466 U.S. 109, 113 (1984), and the Court has also characterized the interception of intangible communications as a seizure. *See Berger v. New York*, 388 U.S. 41, 59–60 (1967). Furthermore, the Court has held that a "search occurs when an expectation of privacy that society is prepared to consider reasonable is infringed." *Jacobsen*, 466 U.S. at 113.

OLE goes on to state that "A search is constitutional if it does not violate a person's 'reasonable' or 'legitimate' expectation of privacy. *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring)."

Another piece of legislation in the United States is the Patriot Act, which provides law enforcement agents with an increased ability to use surveillance tools such as roving wiretaps. The Patriot Act introduced important changes that have increased the prosecutorial power in fighting computer crimes. The Patriot Act references the Computer Fraud and Abuse Act (18 U.S.C. § 1030) with both procedural and substantive changes. There were also changes to make it easier for law enforcement to investigate computer crimes.

Also relevant piece of legislation in the United States is with regard to border searches. According to the Supreme Court, routine searches at the border do not require a warrant, probable cause, or even reasonable suspicion that the search may uncover contraband or evidence.

Similar to the UK's RIPA, since 1968, in the United States, the Wiretap Statute (Title III), 18 U.S.C. §§ 2510–2522 has been the statutory framework used to control the real-time electronic surveillance of communications. When law enforcement officers want to place a wiretap on a suspect's phone or monitor a hacker breaking into a computer system, they have to do so in compliance with the requirements of Title III. The statute prohibits the use of electronic, mechanical, or other devices to intercept a private wire, an oral, or electronic communication between two parties unless one of a number of statutory exceptions applies. Title III basically prohibits eavesdropping (subject to certain exceptions and interstate requirements) by anyone, everywhere in the United States.

e. Hagen E., Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations Computer Crime and Intellectual Property Section Criminal Division Published by Office of Legal Education, Executive Office for United States Attorneys.

In the United States, the Electronic Communications Privacy Act (ECPA) places limitations on the ability of Investigators to intercept and access potential evidence. In Europe, Article 5 of the European Convention on Human Rights gives similar privacy limitations to the ECPA and limits the processing and sharing of personal data both within the EU and with other countries outside the EU.

The Convention on Cybercrime (ETS No. 185), also known as the Budapest Convention on Cybercrime, is an international treaty that was created to try to address the harmonization of national laws relating to computer crime and Internet crimes in order to improve the investigative techniques and increase cooperation between nations. The Convention was adopted by the Committee of Ministers of the Council of Europe on November 8, 2001 and was opened for signature in Budapest, later that month. The convention entered into force on July 1, 2004 and by the end of 2010, 30 states had signed, ratified, and acceded to the convention. These included Canada, Japan, the United States, and the Republic of South Africa. A further 16 countries have also signed the convention but not yet ratified it. The Convention is the only binding international instrument dealing with cybercrime.

The "International Organization on Computer Evidence" is an organization that was established in 1999 and has been working to establish compatible international standards for the seizure of evidence to guarantee the ability to use digital evidence collected by one state in the Courts of another state.

In civil investigations, the relevant laws of many countries restrict the actions that the Investigator can undertake in an examination. Regulations that are in place with regard to network monitoring and the accessing of personal communications or data stored in the network exist in many countries, and the rights of an individual to privacy is still an area which is still subject to decisions in the Courts.

This is intended only to highlight the range of laws and regulations that the Investigator will need to be aware of and that the Forensics Laboratory will need to ensure that have been taken into account when developing the guidelines for operational processes and procedures.

3.1.14 Insurance

The Forensic Laboratory must regularly review its insurance coverage to ensure that it is appropriate for the types of insurance required in the jurisdiction and at a level commensurate with the business undertaken, specific contractual requirements, and the number of employees.

3.1.15 Contingency Planning

This is activity that is undertaken to ensure that suitable and immediate steps can be taken by management and staff in the event of an emergency. The main objectives of contingency planning are to ensure the containment of the incident and to limit any damage or injury or loss and to ensure the continuity of the key operations of the organization. The contingency plan identifies the immediate actions that should be taken and also the longer-term measures for responding to incidents. The process of developing the contingency plan involves the identification of critical resources and functions and the establishment of a recovery plan that is based on the length of time that the enterprise can operate without specific functions. The plan will be a "living document" and will need to be continuously updated to keep pace with changes in regulations, the environment, and the work taking place within the Forensic Laboratory. The contingency plan will need to be documented in straightforward terms and tested at regular intervals to ensure that it is effective and that all of the parties involved understand their roles and responsibilities. Contingency plans are part of business continuity planning. Business Continuity is covered in Chapter 13.

3.1.16 Roles and Responsibilities

The roles of all Forensic Laboratory employees must be defined together with the responsibilities that are related to that role. Specific job roles are given in the relevant chapters relating to the implemented management systems.

3.1.17 Business Objectives

It is common for business objectives to be set in financial terms; however, not all objectives have to be expressed in these terms. Ideally objectives should adhere to the SMART acronym, which describes five characteristics:

- S—Specific;
- M—Measurable;
- A—Achievable;
- R—Realistic;
- T—Time Bound.

Objectives could include the following:

- desired throughput and profit levels;
- amount of income generated;
- value of the business or dividends paid to shareholders;
- quality of customer service;
- innovation.

3.1.18 Laboratory Accreditation and Certification

Accreditation is something that the Forensic Laboratory will normally aspire to achieve at the earliest opportunity. The most widely recognized accreditation is ISO17025. Once accreditation has been achieved, the activities of the Forensic Laboratory will be monitored on a periodic basis by the relevant accreditation body. Once it has been achieved, the Forensic Laboratory must comply with specific criteria relating to the laboratory's management and operations, personnel, and physical plant in order to maintain its accreditation. The criteria and standards address the areas of laboratory administrative practices, procedures, training, evidence handling, quality control, analysis protocols, testimony, proficiency testing, personnel qualifications, space allocation, security, and a number of other topics. The issue of laboratory accreditation and certification is dealt with in much greater detail in Chapter 19.

3.1.19 Policies

The Forensic Laboratory has developed policies that contain clear statements covering all of the major forensic issues, including subcontracting; contacting law enforcement; carrying out monitoring; and conducting regular reviews of forensic policies, guidelines, and procedures. At the top level, the Forensic Laboratory's policies must only allow authorized personnel to carry out their tasks which may include monitoring systems and networks and performing investigations. The Forensic Laboratory may also need a separate policy to cover incident handlers and other forensic roles. There is a requirement for the policies to be reviewed and updated at frequent intervals because of changes in technology or changes to laws and regulations, as well as to take account of new court rulings. The Forensic Laboratory case handling policies must also be consistent with other policies, including policies related to privacy.

3.1.20 Guidelines and Procedures

The Forensic Laboratory has developed and maintains guidelines and procedures for carrying out all tasks relating to processing forensic cases and management systems. These shall be based on the parent organizations policies (if there is a parent organization), consistent with them and all applicable laws. The Forensic Laboratory's forensic guidelines shall include general guidelines for investigations and shall also include step-by-step procedures for performing the routine tasks, such as the imaging of a hard disk or the capturing of volatile data from live systems.

The reason for developing these guidelines and procedures is that they will help to ensure that there is consistency in the way in which material is processed. This will lead to good practices and a consistent approach to tasks within the Forensic Laboratory and will ensure that the cases are all processed to the same standard whether it is anticipated that they will go to the Court or not. It will also ensure that evidence collected, for example, for a case that starts off as an internal disciplinary action into computer misuse, can be used if it discovered that there was a more serious crime that may lead to a prosecution. By using guidelines and policies to ensure consistency, the integrity of any data that is used or results that are created can be demonstrated. The guidelines and procedures will support the admissibility of any evidence produced in the laboratory into legal proceedings.

If tasks are outsourced to external third parties, the way in which the Forensic Laboratory engages with the third party and the way in which they are engaged and the material that is provided to them and recovered from them shall be described in the guidelines and policies. Normally, when a third party carries out work in behalf of the Forensic Laboratory, the contract with the third party will require that they adhere to the Forensic Laboratory's handling and processing standards.

The process of outsourcing is covered in Chapter 14.

Once the guidelines and procedures have been developed, it is important that they are regularly reviewed and maintained so that they remain accurate and represent the current laws, technology, and good practice. The frequency with which they are reviewed and updated will be determined by Top Management and should be regular but may also be influenced by changes in the relevant laws or technologies.

APPENDIX 1 - THE FORENSIC LABORATORY TOR

THE VISION

A short statement, normally of one or two paragraphs, which explains the mandate given to the team and defines the reason for the Forensic Laboratory's creation and its purpose.

SCOPE AND OBJECTIVES

It is essential to define the scope of the work that is to be conducted by the Forensic Laboratory. The ToR should specify the work to be undertaken and the types of deliverables from this work. It should also give timescales for the production of deliverables.

DELIVERABLES

The deliverables of the Forensic Laboratory should be defined. This should not only include the outcome of the investigations but also the internal deliverables such as accounts, audits, and test results and reports.

BOUNDARIES, RISKS, AND LIMITATIONS

This section describes where the process/system/operation of the Forensic Laboratory starts and ends. A statement of the authority delegated to the Forensic Laboratory to implement change and any powers given to it should be included. It is in this section that the systems, policies, procedures, relevant legislation, etc., should be mentioned. The risks should also be detailed.

ROLES, RESPONSIBILITIES, AUTHORITY, ACCOUNTABILITY, AND REPORTING REQUIREMENTS

The Forensic Laboratory policy should clearly define the roles and responsibilities of all people working within the Forensic Laboratory. It shall detail the roles, responsibilities, and functions of each employee and clearly define the authority that is associated with each of the roles. It should also define the accountability associated with each of the roles and the reporting requirements for each role and task. It shall include the actions to be performed during both routine work activities and an incident. The policy shall clearly indicate who is responsible for, and authorized to contact which internal teams and external organizations and under what circumstances.

STAKEHOLDERS

It is important to identify the main stakeholders and their interests, roles, and responsibilities. The stakeholders will include the representatives of the owning organization, Forensic Laboratory employees, Clients and may extend to other parties who have an interest in the efficient running of the Forensic Laboratory.

REGULATORY FRAMEWORK

The legal, institutional, and contractual framework for the operation of the Forensic Laboratory needs to be stated. This should include regulations of regional bodies such as the European Union, Federal (National), State (Provincial), or Municipal Governments, and any legislation or policies and practices that pertain to parent corporations, partnerships, etc.

RESOURCES

The resources identified should include real estate, employees, equipment, and support services. The elements that need to be considered will include the following:

- administrative support;
- available budget;
- employees;
- materials and supplies;
- other supporting functions (e.g., security);
- resources available and how they are to be accessed;
- information processing equipment (business and forensic);
- training requirements and how this will be provided.

WORK BREAKDOWN STRUCTURE AND SCHEDULE

The work breakdown structure is a list of tasks that require action. When the individual tasks are considered together with relevant dependencies and timelines are introduced, then the schedule is created. The work that is to be undertaken by the Forensic Laboratory is broken down into smaller and smaller tasks that eventually become the work breakdown structure. Additional details of task durations and dependencies will be required to aid in the building of the schedule.

SUCCESS FACTORS

Success Factors (SFs), also sometimes referred to as Critical Success Factors, are the measure of those factors or activities required for ensuring the success of the Forensic Laboratory. They are used to identify a small number of key factors that the Forensic Laboratory will need to focus on to be successful. SFs are important as they are things that are capable of being measured and because of this they get done more often than things that are not measured. Each SF should be measurable and associated with a target goal. Primary measures that should be included are aspects such as success levels for areas such as the number of jobs processed in the month and number of hours spent on each task. SFs should be identified for any of the aspects of the business that are identified as vital for defined targets to be reached and maintained. SFs are normally identified in such areas as laboratory processes, staff and organization skills, tools, techniques, and technologies. SFs will inevitably change over time as the business undertaken by the laboratory changes.

INTERVENTION STRATEGIES

These should cover the contingency plans for any emergency and should define what constitutes an emergency.

APPENDIX 2 - CROSS REFERENCE BETWEEN ISO 9001 AND ISO 17025

ISO 9001	ISO 17025
Clause 1	Clause 1
Clause 2	Clause 2
Clause 3	Clause 3
4.1	4.1, 4.1.1, 4.1.2, 4.1.3, 4.1.4, 4.1.5, 4.2, 4.2.1, 4.2.2, 4.2.3, 4.2.4
4.2 1	4.2.2, 4.2.3, 4.3.1
4.2.2	4.2.2, 4.2.3, 4.2.4
4.2.3	4.3
4.2.4	4.3.1, 4.12
5.1	4.2.2, 4.2.3
5.1 a)	4.1.2, 4.1.6
5.1 b)	4.2.2
5.1 c)	4.2.2
5.1 d)	4.15
5.1 e)	4.1.5
5.2	4.4.1
5.3	4.2.2
5.3 a)	4.2.2
5.3 b)	4.2.3
5.3 c)	4.2.2
5.3 d)	4.2.2
5.3 e)	4.2.2
5.4.1	4.2.2 c)
5.4.2	4.2.1
5.4.2 a)	4.2.1
5.4.2 b)	4.2.1
5.5.1	4.1.5 a), 4.1.5 f), 4.1.5 h)
5.5.2	4.1.5 i)
5.5.2 a)	4.1.5 i)
5.5.2 b)	4.11.1
5.5.2 c)	4.2.4
5.5.3	4.1.6
5.6.1	4.15
5.6.2	4.15
5.6.3	4.15
6.1 a)	4.10
6.1 b)	4.4.1, 4.7, 5.4.2, 5.4.3, 5.4.4, 5.10.1
6.2.1	5.2.1
6.2.2 a)	5.2.2, 5.5.3
6.2.2 b)	5.2.1, 5.2.2
6.2.2 c)	5.2.2
6.2.2 d)	4.1.5 k)
6.2.2 e)	5.2.5
6.3.1 a)	4.1.3, 4.12.1.2, 4.12.1.3, 5.3
6.3.1 b)	4.12.1.4, 5.4.7.2, 5.5, 5.6
6.3.1 c)	4.6, 5.5.6, 5.6.3.4, 5.8, 5.10
6.4	5.3.1, 5.3.2, 5.3.3, 5.3.4, 5.3.5
7.1	5.1
7.1 a)	4.2.2
7.1 b)	4.1.5 a), 4.2.1, 4.2.3
7.1 c)	5.4, 5.9
7.1 d)	4.1, 5.4, 5.9
7.2.1	4.4.1, 4.4.2, 4.4.3, 4.4.4, 4.4.5, 5.4, 5.9, 5.10
7.2.2	4.4.1, 4.4.2, 4.4.3, 4.4.4, 4.4.5, 5.4, 5.9, 5.10
7.2.3	4.4.2, 4.4.4, 4.5, 4.7, 4.8
7.3	5, 5.4, 5.9
7.4.1	4.6.1, 4.6.2, 4.6.4
7.4.2	4.6.3
7.4.3	4.6.2
7.5.1	5.1, 5.2, 5.4, 5.5, 5.6, 5.7, 5.8, 5.9
7.5.2	5.2.5, 5.4.2, 5.4.5
7.5.3	5.8.2
7.5.4	4.1.5 c), 5.8
7.5.5	4.6.1, 4.12, 5.8, 5.10
7.6	5.4, 5.5
8.1	4.10, 5.4, 5.9
8.2.1	4.10
8.2.2	4.11.5, 4.14
8.2.3	4.11.5, 4.14, 5.9
8.2.4	4.5, 4.6, 4.9, 5.5.2, 5.5.9, 5.8, 5.8.3, 5.8.4, 5.9
8.3	4.9
8.4	4.10, 5.9
8.5.1	4.10, 4.12
8.5.2	4.11, 4.12
8.5.3	4.9, 4.11, 4.12

Continued

APPENDIX 3 - CONFLICT OF INTEREST POLICY

This policy describes the Forensic Laboratory Conflict of Interest Policy for all work undertaken, including digital forensics, general management consultancy, and regulatory work.

There is no right or wrong approach to handling potential conflicts of interest. Ultimately, the issue is about the application of common sense within a legislative, regulatory, contractual, or ethical framework. The key principles to any effective policy are as follows:

- *Define a conflict of interest in relation to the Forensic Laboratory:* Would there have to be some personal financial or other interest for a Forensic Laboratory employee for a conflict of interest to be considered, or would historical connection to the beneficiary of a decision be sufficient to trigger the procedures;
- *Consider the future likelihood of such conflicts:* Is the conflict of interest likely to be exceptional in which case the employee's membership of the decision-making body is unproblematic, or would it be so frequent that it might be best to consider alternative membership of the council;
- *Agree the method of declaring an interest:* This may be a written declaration completed annually before undertaking a task (project, case, etc.) or may be prior to a meeting, etc.;
- *Agree the method of addressing the conflict:* Again, there are numerous ways of addressing a conflict of interest. The employee in question might absent themselves completely from all consideration or they may participate in the discussion but not the decision. Each case will be decided on the factors involved;

It is the Forensic Laboratory's policy to have an open, transparent, fair, objective, customer-focused, yet accountable process for any possible conflict of interest. The Forensic Laboratory owes contractual duties, as well as a duty of care, to all of its Clients, and this must be observed and complied with, as well as be seen to be observed and complied with;

The aim of this policy is to protect the Forensic Laboratory and all employees from the appearance of an impropriety;

At the start of any the Forensic Laboratory case or assignment, the employees involved must consider the scope of the assignment and consider if they have now, in the past, or in the foreseeable future, any possible conflicts of interest relating to the assignment. These may arise from such issues as:

- personal, or familial involvement, with someone who is involved in the management of the contract of the assignment;
- personal, or familial involvement, with someone who is the subject of a forensic case or assignment;
- a breach of the code of ethics of any professional organization of the organization that any employee on the case or assignment may belong to or be bound by;
- the offer (or acceptance) of any inducement; hospitality; or gift that may impair, limit the extent, rigor, or objectivity in the performance of the assignment, case, or project;
- having a financial interest in the outcome of the case or assignment;
- impaired decisions or actions that may not be in the best interest of the Forensic Laboratory's Client or the Court;
- a perception that the Forensic Laboratory or its employees are acting improperly because of a perceived conflict of interest.

Where a possible conflict is identified after the start of any assignment, it must be brought to the attention of the Laboratory Manager, who has accountability and responsibility for Compliance and Governance, as soon as is practicably possible, and within 24 hours at the maximum. As soon as the conflict is identified, the employee should excuse themselves from any decision taking until the conflict has been resolved. In some cases, it will be necessary for the employee to excuse themselves from any work on the case or assignment. This is specifically the case for forensic work and may be applicable in other assignments, as identified.

In some cases, a "Declaration of Interest Form" will be required to be executed before each assignment, and in other cases, an annual (or regular) declaration will be required.

Where a conflict is declared to the Laboratory Manager, they will take such action as they see fit to both declare and resolve the conflict. This may (and probably will) involve communication with the other parties in the case or assignment. All discussions and decisions shall be regarded as records and be retained and secured appropriately.

All possible or actual conflicts of interest shall be investigated thoroughly, quickly, impartially, and all relevant parties shall be advised of the outcome.

A review of all conflicts and possible conflicts is undertaken at Management Reviews.

This policy is issued and maintained by the Laboratory Manager, who also provides advice and guidance on its implementation and ensures compliance.

All the Forensic Laboratory employees shall comply with this policy.

APPENDIX 4 - QUALITY POLICY

The Forensic Laboratory is committed to good quality practice. The objective for all employees is to perform their

activities in accordance with the Forensic Laboratory standards to ensure that all the products and services provided meet those standards and meet or preferably exceed the Client's expectations.

Management strives to underline this approach in all their day-to-day activities.

Quality at the Forensic Laboratory is measured by Key Performance Indicators (designated as Quality Objectives) which Top Management review and set each year to ensure that the Forensic Laboratory and its employees attain quality standards, and to ensure continuous improvement of the defined Quality Objectives.

Quality is the responsibility of all employees. Each employee shall ensure that they are familiar with those aspects of the Forensic Laboratory's policies and procedures that relate to their day-to-day work and understand how their contribution affects the Forensic Laboratory's products and services.

The Key Performance Indicators which define the Forensic Laboratory Quality Objectives are set out in Planning within the Business in Chapter 6, Section 6.2.2.1.

The scope of the Quality System implemented at the Forensic Laboratory is the whole of the digital forensics operations undertaken.

It is the Forensic Laboratory's policy to:

- only purchase from approved suppliers, who shall be regularly audited, this includes all outsourcing partners (Chapter 14);
- handle all Client feedback, including complaints, in an effective and efficient manner and use them as input to continuously improve the Forensic Laboratory's products and services (Chapter 6, Section 6.14);
- ensure that all agreed Client requirements are met;
- implement a process of continuous improvement (Chapter 4, Section 4.8 and Appendix 14);
- ensure that all employee training needs are identified at a Training Needs Analysis as part of the employee's annual appraisal process or as required (Chapter 4, Section 4.6.2 and Chapter 18, Section 18.2.2).

Where a Client requests that the Forensic Laboratory conform to their own Quality System, the Forensic Laboratory shall apply this system as described in Chapter 6.

This policy is issued and maintained by the Quality Manager who also provides advice and guidance on its implementation and ensures compliance.

All the Forensic Laboratory employees shall comply with this policy.

Intentionally left as blank