Digital Forensics Laboratory

Amira Muaket
Old Dominion University

Professor Bechard

28 February 2025

Summary

Forensic laboratories are crucial when conducting and storing evidence collected from an investigation. When having a lab you must place importance on processes, and policies, and maintain a consistent procedure for everyone to follow. This can ensure your work is reliable and upholds integrity in the process. Following guidelines from the ANSI-ASQ National Accreditation Board (ANAB) and the international standard ISO/IEC 17025:2017. One of the main attributes constructed in this document will provide a physical layout of the lab and description. While including an accreditation plan highlighting the applicable controls when performing laboratory activities. “ISO/IEC 17025 has been developed to promote confidence in the operation of laboratories. This document contains requirements for laboratories to enable them to demonstrate they operate competently and can generate valid results.”(ANAB). Next, providing a maintenance plan, since the lab should be maintained all the time, can ensure the safety and overall health of lab personnel. Following proper protocols can help prevent or minimize any machine failure or unplanned disasters. Next is identifying roles and responsibilities for lab managers and technician requirements for the laboratory.

Lab Accreditation Plan

ISO/IEC 17025:2017 standards are a guideline for any business, organization, or government entity, where they can indulge in stating their goals/purposes, and laboratory layouts, and essentially choose which implements can best suit their needs. It helps specify the required duties and responsibilities that laboratories must uphold. The following are the five main sections that contain the requirements for an accreditation plan:

1. Section 4: States the “General Requirements” which covers both “Impartiality” and “Confidentiality”. These two requirements are important as they assist in maintaining a mutual trust that all information is kept secure and protected. Impartiality in this sense implies that laboratories won't compromise the quality of results. “Confidentiality” requires that all laboratories keep the results and all data/ information related are kept private.
2. Section 5: Revolves around “Structural Requirements”, it clarifies the organizational components of a laboratory from a range of different activities being done. As it follows a management system by emphasizing that a laboratory

"must be a legal entity or part of a legal entity", thus responsible for the testing and calibration. It also provides management responsibilities to ensure the laboratory is following regulations, customers' needs/wants, and recognition.

3. Section 6: With "Resource Requirements", it follows six clauses that direct the requirements for the laboratory, such as "personnel, facilities, equipment, systems, and support services necessary to perform its laboratory activities"(Advisor)
4. Section 7: "Process Requirements" covers 11 processes to assist in improving effectiveness and efficiency. Where the procedure will review requests, tenders, and contracts. It's where verification and validation of methods come into play, where the laboratory will use the appropriate method and procedure depending on the situation.
5. Section 8: "Management System Requirements", this standard depends on the size of your laboratory. If the laboratory is a part of a larger organization or has an effective management system must be in accordance with ISO 9001:2015, as well as, demonstrate its commitments to ISO 17205 clauses 4-7.
6. Below provides the laboratory compliance with the ISO/IEC 17025:2017. As this will serve as a checklist for the accreditation plan. As well as to determine the laboratories competency when it comes to testing and calibration.

Policy Topic	Attachment Number	Submission Examples Required	ISO Reference	Initial	Reaccreditation	FoR Addition
ISO/IEC 17025	6A.1	Are results that were generated by other forensic testing laboratories. As this document provides that laboratories are operating up to standards while providing valuable/reliable results.	All			
Site	6A.2	This list is used to check off all	All			

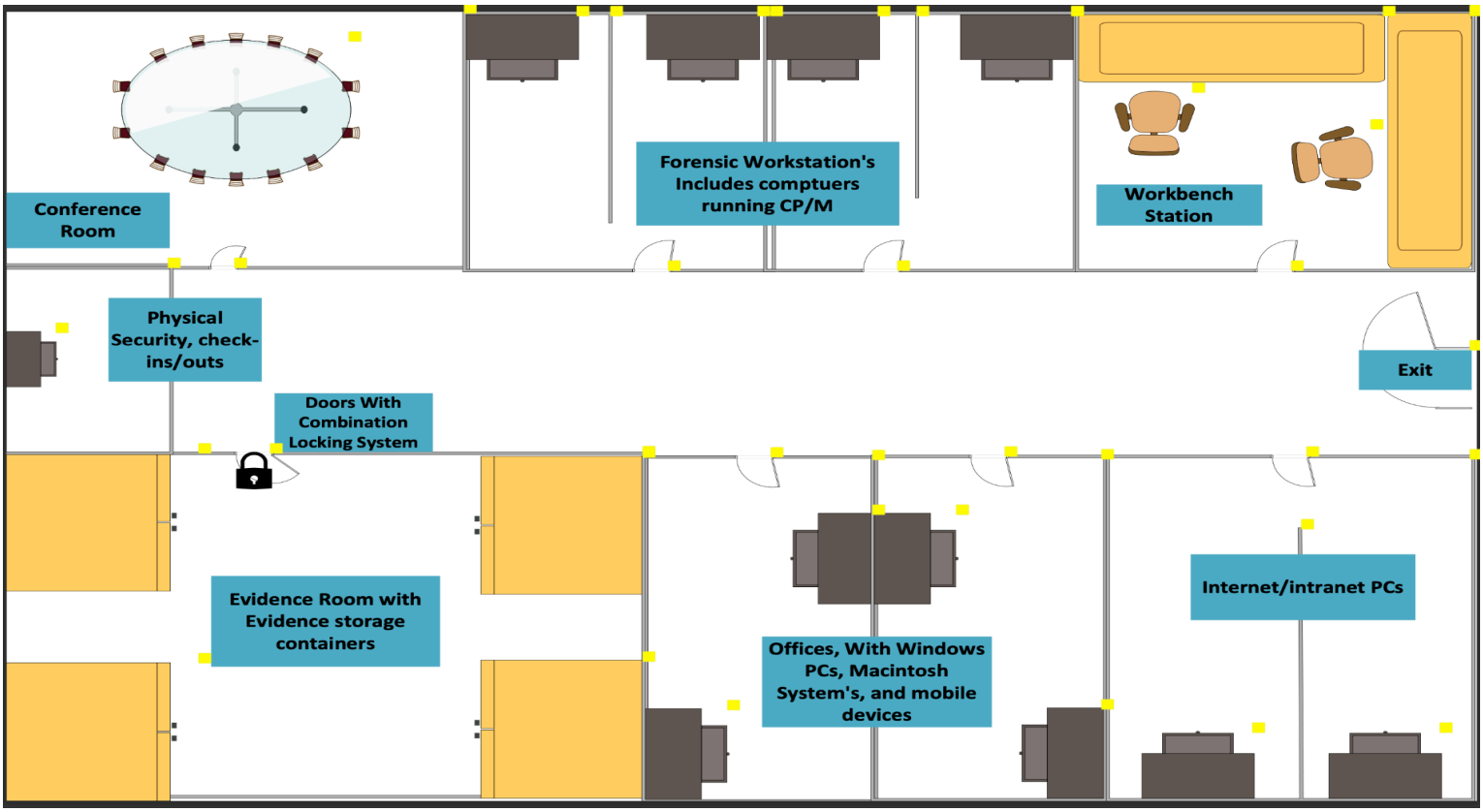
Assessment Checklist		laboratory compliance to the ISO/IEC 17025 standard.				
Organization Chart	6A.3	The laboratory must implement the needed controls for identification, storage, protection, back-up, archive, retrieval, retention time, and disposal of its records. As well as records for periods that are consistent with its contractual obligations.	8.4.2			
Document Control	6A.4	Laboratory must establish documents, maintain policies and objectives. This can ensure that the policies and objectives are acknowledged and implemented at all levels of the laboratory.	8.2.1			
Document Control	6A.5	Laboratory management must provide evidence of commitment to the development and implementation of the management system and to continually improve its effectiveness.	8.3.2		Must be reaccredited	
Corrective Action	6A.6	Laboratory must have records as evidence for: A) the nature of the nonconformities causes and any subsequent actions. B) The results of any corrective action.	8.7.3		Must be reaccredited	
Internal Audit	6A.7	Laboratories must retain records as evidence of the implementation of the	8.8.2e			

		audit program and the audit results.				
Management Review	6A.8	This is inputs to the management's review that will be recorded and include information such as: a)any internal or external changes that are relevant to the laboratory; b) fulfill objective; c) follows policies and procedures; d) status of actions; e) outcome of recent audits; f) corrective actions; g) assessments of external bodies; h) changes in volume or type of work; i) customer and personal feedback; j) complaints; k) effectiveness of any implemented improvements; l) adequacy of resources; m) results of risk identification; n) outcomes of the assurance of the validity of results; o) other relevant factors.	8.9.2		Must be reaccredited	
QA Reports	6A.9	The laboratory must have a procedure for the review of requests, tenders and contracts.	7.7.1			
Facilities	6A.10	The facilities and environmental conditions must be suitable for the laboratory activities. (Laboratory Floor Plans).	6.3		Must be reaccredited	
Test Methods	6A.11	The laboratory will use appropriate methods and procedures for all	7.2.1.1		Must be reaccredited	

		laboratory activities and for evaluation of the measurements uncertainty, and statistical techniques.				
Traceability	6A.12	Metrological traceability is established by considering, and then ensuring, the following: a) the specification of the measurand; b) a documented unbroken chain of calibrations going back to stated and appropriate references; c) that measurement uncertainty for each step in the traceability chain is evaluated according to agreed methods; d) that each step of the chain is performed in accordance with appropriate methods, with the measurement results and with associated, recorded measurement uncertainties; e) that the laboratories performing one or more steps in the chain supply evidence for their	A.3.1			
Uncertainty of Measurement	6A.13	Laboratories must perform a testing shall evaluate measurement of uncertainty. Will conduct a test method so it can preclude rigorous evaluation of measurement uncertainty, thus an estimation will be	7.6.3		Must be reaccredited	

		made based on an understanding of the theoretical principles or practical experience of the performance.				
Final Report	6A.14	The outputs from the management review will record all decisions and actions. A) effectiveness of management system and processes; b) improvements of the laboratory; c) provisions of required resources: d) any need for change.	8.9.3			
Proficiency Testing	6A.15	Computer Forensics Tool Testing Program (CFTT), it establishes a methodology for testing computer forensic software tools.	Module 6			

Forensic Laboratory Floor Plan



Inventory

Hardware	Software
• Computer Chairs (10) • PC Power Cables • 40 IDE Cables • 40 SATA Cables • Secure Storage Room • Cisco 3560 Switch • 40 CAT 6E cables • Fluke Network Cable Tester • Spectrum Analyzer	• Kali Linux • Helix Pro • Autopsy • FTK (Forensic Toolkit) • VIP 2.0 (Video Investigation Portable) • Sleuth Kit • Cellebrite UFED • X-Ways Forensics • Volatility

• PC Component (Adapters, Cables, etc...) • A digital camera capable of still and motion recording • Assorted antistatic bags • An external CD/DVD drive • 40-pin 18-inch and 36-inch IDE cables, both ATA-33 and ATA-100 or faster • Ribbon cables for floppy disks • Extra USB 3.0 or newer cables and SATA cards and associated cables • Extra SCSI cards, preferably ultrawide • Graphics cards, both Peripheral Component Interconnect (PCI) and Accelerated Graphics Port (AGP) • Assorted FireWire and USB adapters • A variety of hard drives and USB drives (as many as you can afford and in as wide a variety as possible) • At least two 2.5-inch adapters from notebook IDE hard drives to standard IDE/ATA drives, SATA drives, and so on • Computer hand tools, such as Phillips and flathead screwdrivers, a socket wrench, any vendor-specific tools, a small flashlight, and an antistatic wrist strap • Sources (Module 2 Readings)	• Magnet AXIOM • OS Forensics • Paladin Forensic Suite

Roles/Responsibilities

Having proper staff is crucial for a forensic laboratory, it must have Lab managers and technicians. According to the ANAB, each forensic laboratory must have a specific objective

carried out by the lab manager. Their duties include setting up various processes depending on the cases, and reviewing them regularly. Must perform general management tasks such as creating group consensus in decision making, enforcing rules and regulations, updating the laboratories for new hardwares/software, and ensuring the facilities are up to date. Their roles also include estimating how many cases each investigator can handle, while creating and monitoring laboratory policies for staff and evidence.

Laboratory technicians roles revolve around “forensic collection, recovery, processing, preservation, analysis, storage, maintenance, and/or presentation of digital evidence.”(Hillsboro) Usually someone in this field must have knowledge that centers on hardware and softwares, such as OSs and file types. Must be updating on the latest technical trends, so they can enhance their investigative and computer skills. Maintain up-to-date library resources such as software, hardware, information and technical journals.

Maintenance Plan

A maintenance plan is required for laboratories to uphold to ensure safety. The Laboratory Manager, Quality Assurance Liaison, or designee will ensure that each unit maintains a record of instruments and equipment that require calibration. This record will include, at a minimum: the identity of the item of equipment and its software; the manufacturer’s name and type identification. We can also observe the ISO/IEC 17025:201 sections: 5.6, 6.4.3, 6.4.13g, and 6.6.1 all mention a type of maintenance, wherever it is structural, facilities, equipment, products, and services.

Facility maintenance is highly critical, if there's any damages in the laboratory, wherever if its physical or technical must be repaired immediately. Allowing escort cleaning crews while watching them is highly recommended. Since a lot of laboratories will have static electricity, if not handled properly can put others at risk. It’s a good practice to have two separate trash containers, one for regular trash (non-related to the investigation) and one for sensitive materials.

Bibliography

Job Descriptions | Career Opportunities. (n.d.). Www.governmentjobs.com. https://www.governmentjobs.com/careers/hillsboro/classspecs/862521

Aguilar, J., Barnes, T., Browne, J., Kennedy, A., Miranda, R., Williams, S., Burney, Y., Byrd, J., Carver, B., McClaren, J., McElroy, R., Denmark, A., Mount, M., Halla, S., Hartman, L., Mohr, K., Leben, D., Matheson, G., Sigel, S., & Smither, J. (2013). Forensic science laboratories : handbook for facility planning, design, construction, and relocation. https://doi.org/10.6028/nist.ir.7941

General requirements for the competence of testing and calibration laboratories exigences générales concernant la compétence des laboratoires d'étalonnages et d'essais. (n.d.). https://www.iasonline.org/wp-content/uploads/2021/02/ISO-IEC-17025-2017-IAS.pdf

ISO 17025 documentation requirements: What is mandatory? (n.d.). Advisera.com. https://advisera.com/17025academy/blog/2019/08/30/list-of-mandatory-documents-required-by-iso-170252017/

ISO 17025 – Main guidelines. (n.d.). 17025Academy. https://advisera.com/17025academy/what-is-iso-17025/

ISO/IEC 17025 (2023). Forensic Calibration Accreditation. ANAB. https://anab.ansi.org/accreditation/iso-iec-17025-forensic-calibration/

ISO/IEC 17025 - ANAB. (2023). ANAB. https://anab.ansi.org/standard/iso-iec-17025/?srsltid=AfmBOoov1qPURnEqPdLmuarS9vU29X9DzMKvfiSHbmltNipTiJoPHNpG

Setting Up a Forensic Lab: Key Components and Best Practices. (2024, June 19). https://www.salvationdata.com/knowledge/forensic-lab/

10 Useful Digital Forensics Software in 2023. (2023, August 11). SalvationDATA Technology. https://www.salvationdata.com/knowledge/digital-forensics-software/

Allen, T. (2017, May 8). Computer Forensics Tool Testing Program (CFTT). NIST. https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cftt