Digital Forensics Laboratory Accreditation and Maintenance Plan

Kevin Durand

CYSE 407

Old Dominion University

1. Overview

In order to maintain a lab in such a way that it is productive and maintains certain levels of conformity to excellence and proper functionality. Accreditation will be carried out, adhering to the auditing and accreditation standards of the International Standard ISO/IEC 17025:2005 accreditation. In order to maintain the necessary standard of the ISO/IEC 17025:2005, there are number of situations that need to be attended to and carried out, expressing the basic needs of accreditation for the 17025 standard in the form of a table will ensure correct completion and understanding of all steps needed to achieve accreditation. A physical layout will be made, along with required equipment, to create the laboratory to function as needed, there will be a certain number of equipment laid out in a proper way to ensure safety and function of the equipment and personnel there within. Staff, with certain duties and requirements are laid out in order to properly man the laboratory, and will enact certain responsibilities as required by the lab. Maintenance along with proper auditing procedures will be written out, to ensure safe and secure lab operations for the equipment, evidence, and personnel there within.

2.Accreditation

To begin an accreditation for a digital forensic lab for International Standard ISO/IEC 17025:2005 a lab must apply for “General Requirements for the Competence of Testing and Calibration Laboratories” and provide evidence of ownership of this document prior to applying for accreditation. This plan will use the ANAB and ISO 17025:2005 standards for accreditation. The following steps will be used to start the accreditation process:

a. For initial laboratories only: The laboratory must submit required application and/or proof of:

   According to “Accreditation Manual” 2023, ANAB Accreditation manual International Standard ISO/IEC 17025:2005 requirements necessitate the collection of the following documents.

   · A licensed copy of the international standard, if applicable to the Program for accreditation (e.g., ISO/IEC 17025 for testing/calibration, ISO/IEC 17020 for inspection)
   · This MA 3033 accreditation manual
   · Accreditation scheme Requirements (AR 3125 for testing/calibration, AR 3120 for inspection, AR 3181 for property and evidence control units)
   · Application and draft scope documents
   · If applicable, additional requirements (e.g., FBI Quality Assurance Standards, ABFT Forensic Toxicology Laboratory Accreditation Checklist, MD OHCQ)

Upon collection of those documents there are a few more steps before accreditation can be reached; certification of receiving documents is required, as ownership of documents required needs to be certified and that certification needs to be emailed to QualityMatters@anab.org. Next a document of conformance is sent by ANAB, checklists and tools will be sent, so that conformance will be met before accreditation assessment begins. Upon completion of the pre-conformance checks and auditing to ensure conformance, the application for assessment will be sent to ANAB. A site visit will be carried out by ANAB to, review documentation and identify missing components, review conformance requirements, and provide a written report on findings.

b. Completion of indicated sections of the site assessment checklist and submission of the following documentation is required, as discussed above. First document that is required for the site assessment checklist is that the site confirm that it has the required documentation on ISO/IEC 17025:2005. The accreditation scheme paper work requires the following checklists to be followed, AR 3125, 3120, and 3181, these documents are the accreditation requirements put forth by ANAB. After everything is gathered together, there is a confirmation of documentation and then official application needed to begin the accreditation process.
c. Contact the ANSI-ASQ National Accreditation Board (ANAB) website for information on accreditation fees at http://www.anab.org/lab-related-accreditation/request-for-quote
d. Forensic service providers who have already begun preparing for accreditation under a previous application may begin again, if they have applied for inactive status, or have been put on suspended status. Inactive status is granted when the applicant removes themselves from the process for unforeseen circumstances, and suspended status is when the applicant needs to fix something in order to be allowed to continue the process. For an inactive applicant, one year is given before movement has to be made on the application but will not exceed the accreditation certification and scope. Suspended status will last for six months but will not exceed the accreditation certification and scope, for this status once the applicant has made the necessary changes the suspension is removed and the process continues.

3. The Laboratory must be familiar with and comply with all relevant ISO/IEC 17025:2005. The table below serves as a sample for the ISO checklist for an accreditation application. The necessary steps for accreditation are listed below in Table 3.1: ISO/IEC 17025:2005 Checklist.

Table 3.1: ISO/IEC 17025:2005 Checklist

Policy Topic	Attachment Number	Submission Examples Required	ISO Reference	Initial	Reaccreditation	FoT Addition
ISO/IEC 17025	6A.1	By gathering the documents, covered in section 1, and conforming to the accreditation standards, accreditation is gained and a final report is written up.	All			
Site Assessment Check	6A.2	After an opening meeting with the accreditation assessment team. 1. Witnessing:sample of personnel performing authorized tasks 2. Interviews:sample of personnel covered 3. Document and record review: sample of documents needed Corrections are made as needed, in areas lacking conformance Results of assessment will be discussed. A closing meeting is had with the applicant(s).	All			
Organization Chart	6A.3	Policy statements: organization's purpose and strategic direction. Individual strategy documents. Records of contextual meetings Risk assessment of internal/external issues	ISO 4.1.5e			
Document Control	6A.4	Laboratory shall establish and maintain procedures to control all documents that form part of its management system. Regulations, Standards, other normative documents.	ISO 4.3.1			
Corrective Action	6A.5	Determine cause and extent of nonconformance. Take appropriate action to eliminate the causes of nonconformity Evaluate effectiveness of steps	ISO 4.3.2.1		Conducted as needed	
Preventative Action	6A.6	Prevent reoccurrence of nonconformity resulting in corrective action requirements.	ISO 4.9.1, 4.11.1		Conducted as needed	
Internal Audit	6A.8	Conformity to Inspection body requirements ISO/IEC 17025 requirements AR 3120 Document conformance	ISO 4.12.2		Conducted Annually	
Management Review	6A.9	Changes in internal/external issues relevant to property/evidence tasks Adequacy of Policies and Procedures Internal Audit outcomes	ISO 4.14.3, 2A.14.1		Conducted Annually	

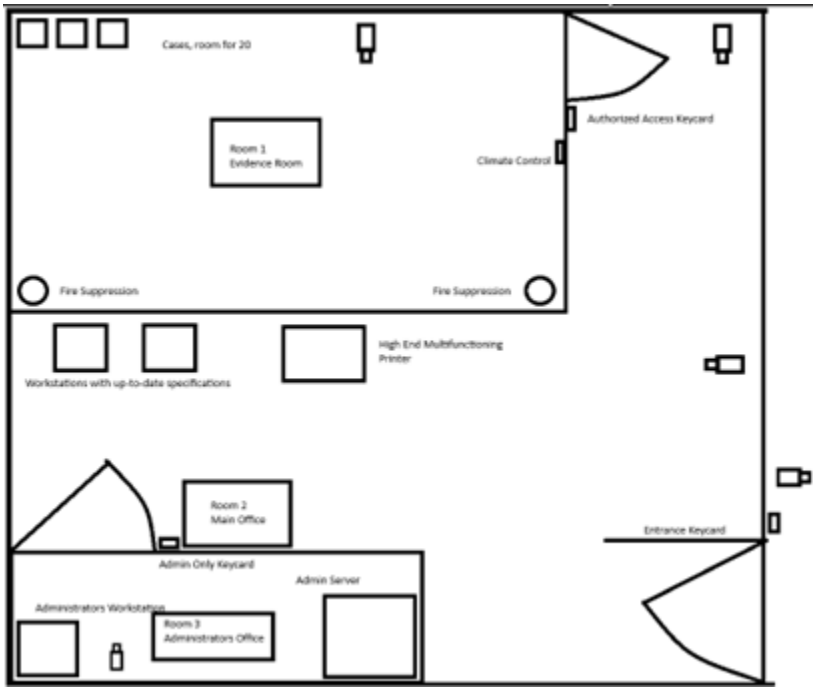
		Personnel review				
QA Reports	6A.10	Quality Assurance on all Auditing and Reviews	ISO 4.15.2		Conducted Annually	
Facilities	6A.11	Record environmental conditions of the facilities, within acceptable limits	2A.4.15.2		Conducted as needed	
Test Methods	6A.12	Proficiency testing the calibration and any check of the calibration status shall be carried out by appropriately trained, competency tested, and authorized personnel	2A.5.3		Conducted as needed	
Traceability	6A.13	Metrological traceability Measurement results by utilizing products and services for measuring equipment for reference standards	ISO 5.4.1		Conducted as needed	
Uncertainty of Measurement	6A.14	the inspection body shall have and apply a procedure for calculating the measurement uncertainty for each equipment calibration it conducts With a review as needed	ISO 5.6		Conducted as needed	
Final Report	6A.15	A final report will be tendered following the end of the accreditation assessment. This report will cover the nonconformities found in the facility/organization and how those were dealt with	ISO 5.4.6, 5.10.3.1c			
Proficiency Testing	6A.16	evaluation of participant performance against pre-established criteria by means of interlaboratory comparisons	Module 6			

4. Physical Layout

In order to carry out all the tasks that will be performed and needed in the Forensics Lab, the proper lab set up must be made; in making the correct Forensics Lab enough equipment is needed to store the data recovered with enough computing power to carry out those tasks in a timely manner, along with making sure enough security and fire prevention is put in place. Starting with the storage, the room will require a storage area capable of containing 20 cases, this area will have a climate-controlled area with a fire suppression system, as seen is Figure X.1. Room 1, additionally there will be room for physical evidence that can not be stored as digital evidence. The next area will be the main office area, Figure X.1. Room 2, in this room there will be two workstations with the latest software and computer specifications and a multi-functional

printer; in addition to the computers and printers there will be an atrium that has a door locked using a secured keycard access, there will be multiple security cameras around the room, documenting everything that happens in that room. Lastly there will be an administrative office, this is where the computers used for decrypting or other work are administered from, additionally the server found in the office will control and store everything the cameras record. Keycard access in this office will be as follows, everyone working in the office and the maintenance staffed cleared to keep the room clear will have access to the main door, only authorized individuals are allowed to access the evidence room and temporary access will be given, lastly the administrative office will only be accessible to the administrator(s). Additional devices, not shown in Figure X.1 will be added, these devices will include an integrated fire detection system that will be made as computer safe as possible, the second device not shown in this room is an intrusion detection system such as a home might contain.

Figure 4.1: Forensics Office



The room, as shown in Figure X.1 is the administrative office, containing all the rooms needed to carry out the requisite tasks, there are a few things that have more requirements than shown in Figure X.1. In the evidence room there will be a storage device for all things that need to be accessed later, or are unable to be stored on a computer, this is to make sure that all evidence is behind a locked door and only accessible on a need-to-know basis. The workstations

in Room 2, Figure X.1. will be the most up-to-date versions of Windows, with a Linux and MacOS virtual machines, with the most recent versions of applicable software all included on a high-performance machine. Physical security is of upmost importance and many steps are made to keep the office secure, with special regards to areas within the office itself. The main entry way will be equipped with two separate doors, the first door is to make sure access is granted to those with access without showing the inside operations of the room itself, as well as a second door with another keycard entry for full access. Inside the main entry, after the main entry door and before the secondary entry, will contain the alarm system panel, the first person in will disengage the alarm, but not the door entry indicator, and the last person out will reengage the alarm again. For extra security areas more security is required, both the administrator's office and evidence room will be kept behind a separate keycard access, only allowed to the administrator(s) or anyone who needs to get into the evidence room.

[*This space left intentionally blank*]

5. Hardware and Software

There are a number of things that are required to have, for in office and at location services. Hardware, while this list is not exhaustive, will include things for the office, such as the workstations and the software they contain. In addition there will be equipment used for on-site operations, mostly for the removal and constructive deconstruction of devices found at site locations. SSA, McDonald J.P. recommends a number of things to have on hand, from his time in and training the FBI.

Table 5.1

Hardware	Software
1. Forensic Workstations (2)	1. Digital Imaging Tools
2. Evidence Storage Unit Cases (20)	2. Forensics Toolkit and Licenses
3. Server Rack	3. Encase Software and Licenses
4. Network Switches (2)	4. Wireshark
5. Intrusion Detection System	5. Autopsy Software and Licenses
6. Backup Power Supply (UPS)	6. EvidenceOnQ Software
7. Write Blockers (2)	7. Clio, Case Management Software
8. Hardware Tools	8. Caseworks, Evidence Management
10. Cell Phones/PDA	9. File Carving Tools
11. Faraday Bags/Carrying Case	10. Encryption/Decryption Software
12. Tape Drives	11. Imaging Tools
13. Various Cables	12. Hash Calculator tools
14. Flashlight	13. Anti-Malware/AntiVirus
15. Printer Cartridges	
16. Evidence Packaging Materials	

6. Maintenance Plan

These practices establish calibration and maintenance requirements to ensure accuracy and reliability of data and evidence collected by the facility and the applicants. Labs should maintain a certain level of safety and health for the facility and its personnel. Any facility maintenance or cleaning crews are to be escorted by a member of the personnel and should be monitored during the completion of their work. Static electricity should be dealt with during any cleaning procedure, maintain a neutral charge on all surfaces and any carpeting that should be done. Maintaining two separate containers for trash that is normal, such as empty disks or other trash, and another container for the correct displacement of sensitive material(s).

7. Roles/Responsibilities

The staff, at any time, will be maintained with one member of management to two working staff members under their direction.

The Laboratory Manager, Quality Assurance Liaison, or Designee will:

Is the main point of contact for processes for managing, setting up, and reviewing cases. Establishes and promotes quality assurance in the laboratory. As a general management professional will promote group consensus on thinking, ethical standards, and making fiscal responsibility for the lab. Promotes and maintains procedures on a safe and secure facility. Oversees Lab staff, encouraging and promoting an efficient working environment. In addition to all other practices, the Lab Manager will make sure to have management over interactions with the law enforcement that it serves, review and maintain a sound budget, and ensure the staff adheres to standards.

Lab Staff will be composed of individuals with working knowledge of the subject, maintaining personal certifications that are required for the operation of the equipment or procedures needed by the lab operations. Staff will follow the direction of Laboratory Management, making sure their actions are carried out to maintain a safe and secure working environment. Staff will make sure to maintain their work stations and action in such a way that keeps equipment and procedures working properly.

Qualifications for all laboratory facility personnel will be regularly tested and maintained at all levels of the organization.

8. Maintenance Practices

The Laboratory Manager, Quality Assurance Liaison, or The Laboratory Manager, Quality Assurance Liaison, or designee will ensure that each unit maintains a record on 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, type identification, calibration

results, time of last calibration, acceptable limits of deviation on the equipment. Regular equipment practices will be carried out, to ensure the viability, usability, and precision of equipment there within. Workstations will be kept clean, safe from charges, and up-to-date with the latest software and firmware updates. The lab will maintain data in such a way that is kept safe and recoverable, a number of tests will be done to reaffirm the safety of the data. In addition to the safe storage of data, is the reassurance of recoverability of data, the site will maintain testing to ensure recoverability of data. In addition to the securing of data and equipment the site will maintain a safety and security conformity, auditing on the safety and security of the lab will be carried out regularly, and its results collected. The lab will maintain a cleanliness to prevent damage to the equipment or contamination of data or evidence collected. In addition to maintaining a dust free environment, the lab itself will also maintain clear carpets and flooring, and that all preventative measures are in working order.

Lab equipment will undergo regular calibration testing and upgrades, as needed or required by the accreditation or reaccreditation auditing team. Equipment will be tested within certain parameters of precision and in working order, carry out audits and testing regularly to ensure the equipment exists within working standards. Upgrades to existing equipment will be carried out regularly, maintaining equipment to be within the best software and hardware updates, especially in regards to keeping workstations and servers up and running. Equipment will be replaced as needed, making sure to maintain a requisite number of pieces in a certain working order, equipment that is not up to standard will be removed and newer or working replacements will be provided.

[*This space left intentionally blank*]

References

1. Nelson B. et. al. (2019). *Guide to Computer Forensics and Investigations: Processing Digital Evidence.* Cengage Learning

2. SSA, McDonald J.P. (Accessed: Nov 24 2023). *Building a Basic Computer Forensics Laboratory.* FBI. Philadelphia Office. https://www.oas.org/juridico/spanish/cyber/cyb32_forensics_lab_en.pdf

3. Accreditation Requirements for Forensic Testing and Calibration (2023). Retrieved from AR 3125 (qualtraxcloud.com)

4. Accreditation Manual for Forensic Laboratories, Forensic Inspection Bodies, and Property and Evidence Control Units (2023) Retrieved from MA 3033 (qualtraxcloud.com)

5. Terms and Conditions for Accreditation (2023) Retrieved from AG 1008 (qualtraxcloud.com)

6. Accreditation Requirements for Forensic Inspections (2023) Retrieved from AR 3120 (qualtraxcloud.com)

7. Accreditation Requirements for the Management and Operation of Property and Evidence Control Units (2023) Retrieved from AR 3181 (qualtraxcloud.com)