FORENSICS LAB ACCREDITATION PLAN FOR MEDIUM SIZED POLICE STATION

Jeggo Paolo V. DyCok

Summary

The ISO/IEC 27037:2012 standard offers detailed instructions for handling digital evidence, including its identification, collection, acquisition, and preservation. It is a crucial tool for businesses of all kinds, including police departments, who need to guarantee the accurate and legal management of digital evidence in court. The standard applies to a wide range of things, including digital storage media, mobile devices, network devices, and digital cameras. Organizations can contribute to ensuring that digital evidence is handled and analyzed in a way that is dependable, admissible, and helps law enforcement investigations and prosecutions by adhering to the ISO/IEC 27037:2012 standard.

Accreditation Plan

This plan outlines the steps that will be taken to achieve ISO/IEC 17025:2017 accreditation for the [Lab Name] laboratory.

1. **Select an accreditation body.** The American National Accreditation Board (ANAB) is a reputable and well-respected accreditation body that offers ISO/IEC 17025:2017 accreditation for forensic laboratories.
2. **Review the accreditation requirements.** Visit the ANAB website to learn more about the ISO/IEC 17025:2017 accreditation requirements for forensic laboratories.
3. **Submit an application.** Download the ANAB accreditation application form and complete it. Be sure to include all of the required documentation, such as your laboratory's policies and procedures, equipment list, and staff qualifications.
4. **Pay the application fee.** The ANAB application fee for ISO/IEC 17025:2017 accreditation is $3,000.

The following are approved accreditation organizations for forensic laboratories in the US:

- American Association for Laboratory Accreditation (A2LA)
- American National Standards Institute National Accreditation Board (ANAB)
- American Society of Crime Laboratory Directors/Laboratory Accreditation Board (ASCLD/LAB)

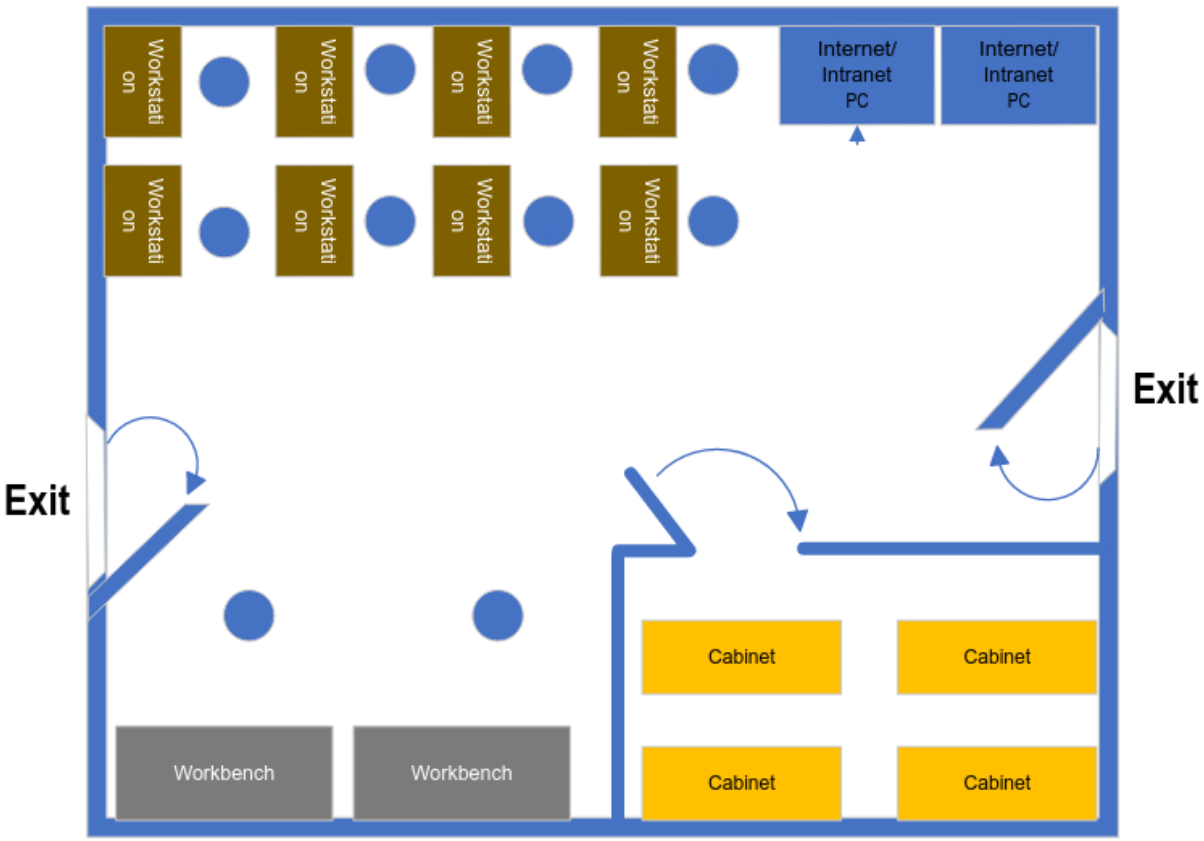
The Laboratory must comply with all requirements relevant to ISO/IEC 17025:2017. The table below shows the checklist for accreditation application. The required steps for accreditation are listed below.

Policy Topic	Submission Examples Required	ISO Reference	Initial	Reaccreditation	FoT Addition
ISO/IEC 17205	Policy statement, procedures for implem	ISO/IEC 17205:2017			

	enting ISO/IEC 17205				
Site assessment checklist	Site assessment checklist	ISO/IEC 17025:2017, section 5.4.2			
Document control	Policy statement, procedures for document control	ISO/IEC 17025:2017, section 5.4.4 AR 3125 7.11			
Corrective action	Policy statement, procedures for corrective action	ISO/IEC 17025:2017, section 5.4.5 / AR 3125 8.7			
Internal audit	Policy statement, procedures for internal audit	ISO/IEC 17025:2017, section 5.4.7 / AR 3125 8.8			
Management review	Policy statement, procedures for management review	ISO/IEC 17025:2017, section 5.4.8 AR 3125 7.11			
QA reports	Sample QA reports	ISO/IEC 17025:2017, section 5.4.9 AR 3125 7.7			
Facilities	Procedures for maintaining facilities and a policy	ISO/IEC 17025:2017, section 5.4.10 / AR 3125 6.3			

Test Methods	Policy and guidelines for creating, approving, and using test methods	ISO/IEC 17025:2017, section 5.4.11 / AR 3125 7.2			
Traceability	Procedures and a policy statement for assuring measurement traceability	ISO/IEC 17025:2017, section 5.4.12 / AR 3125 6.5.			
Uncertainty of Measurement	Statement of policy and guidelines for assessing and disclosing measurement uncertainty	ISO/IEC 17025:2017, section 5.4.13 AR 3125 7.6.3.1			

Forensic Laboratory Floor Plan



Hardware

- **Forensic workstations:**
  - High-performance computer with a powerful CPU, a large amount of RAM, and a large amount of storage space
  - Multiple monitors
  - Docking station for connecting multiple devices
- **Write blockers:**
  - Hardware write blockers for different types of digital storage devices, such as hard drives, USB drives, and memory cards
- **Forensic imaging devices:**
  - Standalone forensic imaging devices
  - Forensic imaging software for use on forensic workstations
- **Mobile device forensics tools:**
  - Mobile device forensic hardware tools, such as JTAG programmers and chip-off readers
- **Other hardware:**
  - Printers
  - Scanners
  - Evidence storage devices, such as external hard drives and tape drives
  - Faraday cages
  - Microscopes
  - Digital camera
  - Assorted antistatic bags
  - External CD/DVD drive
  - 40-pin 180inch and 36 inch IDE cables, both ATA-33 and ATA-100 or faster
  - Ribbon cables for floppy disks
  - SCSI cards
  - Graphics cards
  - Assorted Firewire
  - Assorted Hard drives

Software

- **Operating Systems**
  - Windows 11
  - Kali linux
  - MAC OS
- **Forensic analysis tools:**
  - Autopsy
  - EnCase Forensic
  - FTK Imager
  - X-Ways Forensics
- **Data recovery tools:**
  - GetDataBack
  - R-Studio
  - UFS Explorer

- **Mobile device forensics tools:**
    - Cellebrite UFED Touch
    - AccessData FTK Imager for Mobiles
    - X-Ways Forensics Mobile
- **Network forensics tools:**
    - Wireshark
    - Tcpdump
    - Xplico
    - Kismet
    - Snort

A digital forensics lab needs to have a maintenance plan in place to make sure that its hardware and software are working correctly and that the data is secure. For successful digital forensics investigations to be supported, a well-maintained lab is required to generate accurate and dependable data.

Maintenance Plan

The following is a sample maintenance plan for a digital forensics lab:

- **Hardware maintenance:**
    - Clean the workstations, write blockers, forensic imaging devices, mobile device forensics tools, network forensics tools, and other hardware regularly to remove dust and debris.
    - Update the operating system and software on the forensic workstations frequently
    - Inspect the hardware for any signs of damage or failure.
- **Software maintenance:**
    - Update the forensic analysis tools, data recovery tools, mobile device forensics tools, and network forensics tools regularly.
    - Check the software for any signs of damage or failure.
    - Back up the lab's data regularly.
    - Test the backup system regularly to make sure that it is working properly.
- **Other maintenance tasks:**
    - Keep the lab clean and organized.
    - Train the lab's staff on the latest digital forensics techniques and procedures.
    - Have the lab's equipment calibrated and serviced regularly by a qualified technician.

Roles and Responsibilities

The ISO/IEC 17025:2017 standard is an international standard that specifies the general requirements for the competence of testing and calibration laboratories. The standard can be applied to all types of laboratories, including digital forensics laboratories. With the lab being medium sized, certain employees may hold multiple roles.

According to ISO/IEC 17025:2017, the following roles and responsibilities are essential for a digital forensics lab:

Lab manager:

- **Job description:** The technical manager is in charge of the laboratory's overall technical operation. This includes making that the laboratory has the staff, tools, and resources required to carry out its tasks effectively. Additionally, the technical manager is in charge of creating and implementing laboratory policies and procedures and making sure that the facility complies with all applicable laws and regulations, such as ISO/IEC 17025:2017 and the related policies and procedures of the police department..
- **Requirements:** Master's degree in computer science, information security, or a related field, 5+ years of experience in digital forensics, and experience in managing a team of digital forensics examiners and analysts.

Quality manager:

- **Job description:** The quality manager is in charge of the laboratory's quality management system. This entails creating, putting into practice, and maintaining the system, as well as making sure it works effectively to raise the performance of the laboratory. The quality manager is also in charge of managing the corrective action procedure and conducting internal audits of the laboratory.
- **Requirements:** Bachelor's degree in quality management, information security, or a related field, 3+ years of experience in quality management, and experience in auditing digital forensics laboratories.

Digital forensics examiners and analysts:

- **Job description:** Examiners and analysts who specialize in digital forensics are tasked with gathering, conserving, reviewing, and interpreting digital evidence from a range of devices, including PCs, mobile devices, and servers. They locate and recover deleted or concealed files, extract and examine data from databases and other electronic documents, examine network traffic and logs, prepare reports and present their findings to investigators and other stakeholders, and provide testimony in court regarding their findings.
- **Requirements:** Bachelor's degree in computer science, information security, or a related field, 2+ years of experience in digital forensics, and certifications in digital forensics, such as the Certified Forensic Examiner (CFE) or the EnCase Certified Examiner (EnCE).

Technical support staff:

- **Job description:** The technical support team helps the examiners and analysts of digital forensics. This could involve activities like gathering evidence, using forensic instruments, and maintaining lab equipment.
- **Requirements:** Associate's degree in computer science, information security, or a related field, and 1+ year of experience in digital forensics or a related field.

Administrative staff:

- **Job description:** The laboratory receives administrative help from the administrative team. This may entail activities including scheduling appointments, managing paperwork, and taking calls.
- **Requirements:** High school diploma or equivalent, and 2+ years of experience in administrative work.

References

ANSI National Accreditation Board. (2023, February 1). Accreditation Requirements For Forensic Testing and Calibration (2023).

ANSI National Accreditation Board. (2023, January 13). *Cred-PR-522*. Fees - Accreditation of Credentialing Programs. https://anabpd.ansi.org/Accreditation/credentialing/certificate-issuers/DocumentDetail?DRId=71063

ANSI National Accreditation Board. (2023, January 18). Accreditation Manual For Forensic Laboratories, Forensic Inspection Bodies, and Property and Evidence Control Units.

Nelson, B., Phillips, A., & Steuart, C. (2019). The Investigator's Office and Laboratory. In *Guide to Computer Forensics and Investigations* (6th ed.). essay, Cengage Learning.