Midterm

CYSE407: Digital Forensics

Steven Day

01215086

10/10/2024

Summary

ISO/IEC 17025:2017 establishes the essential framework for the competency of testing and calibration laboratories. This standard is crucial for laboratories seeking to demonstrate their ability to produce reliable and accurate results. In numerous countries, ISO/IEC 17025:2017 has replaced earlier versions and is now the standard for laboratory accreditation, ensuring that organizations meet international quality standards. Accreditation to this standard is important, as many clients and regulatory groups will not recognize testing or calibration outcomes from laboratories that lack this certification.

Accreditation Plan

For new laboratories seeking accreditation under ISO/IEC 17025:2017, the following steps must be taken to initiate the process:

1. **Submission of Required Application**: The lab needs to fill out and send a formal application to the accreditation organization they've chosen, like the ANSI-ASQ National Accreditation Board (ANAB). In this application, the lab must include specific details about what services it offers, how it manages quality, and its technical skills. Additionally, the lab must show that it has the ISO/IEC 17025:2017 standard document, as this is important for the accreditation process.
2. **Completion of the Site Assessment Checklist**: After the lab sends in its application, it must fill out a site assessment checklist that the accreditation organization provides. This checklist helps confirm that the lab's facilities, equipment, and procedures follow the standards set by ISO/IEC 17025:2017. The lab must submit this completed checklist for review before the on-site inspection takes place.
3. **Notification of ANAB Accreditation Requirements**: The lab needs to stay updated with the latest accreditation requirements from ANAB, especially those related to forensic science testing and calibration. These requirements include important guidelines for handling evidence, security measures, and ensuring that forensic analysts have the right skills and knowledge.
4. **Consultation for Accreditation Fees**: The lab should reach out to ANAB (or another relevant accreditation organization) to find out about the costs involved in getting accredited. This includes fees for the initial application, document reviews, site assessments, and regular check-ups after accreditation.
5. **Continuity for Existing Forensic Service Providers**: Forensic labs that have already started the accreditation process based on older guidelines should keep following the steps they've been using. They also need to make sure that their systems and procedures are updated to comply with the ISO/IEC 17025:2017 standard, as well as any new requirements from the accreditation organization.

List of Approved Accreditation Organizations in the US:

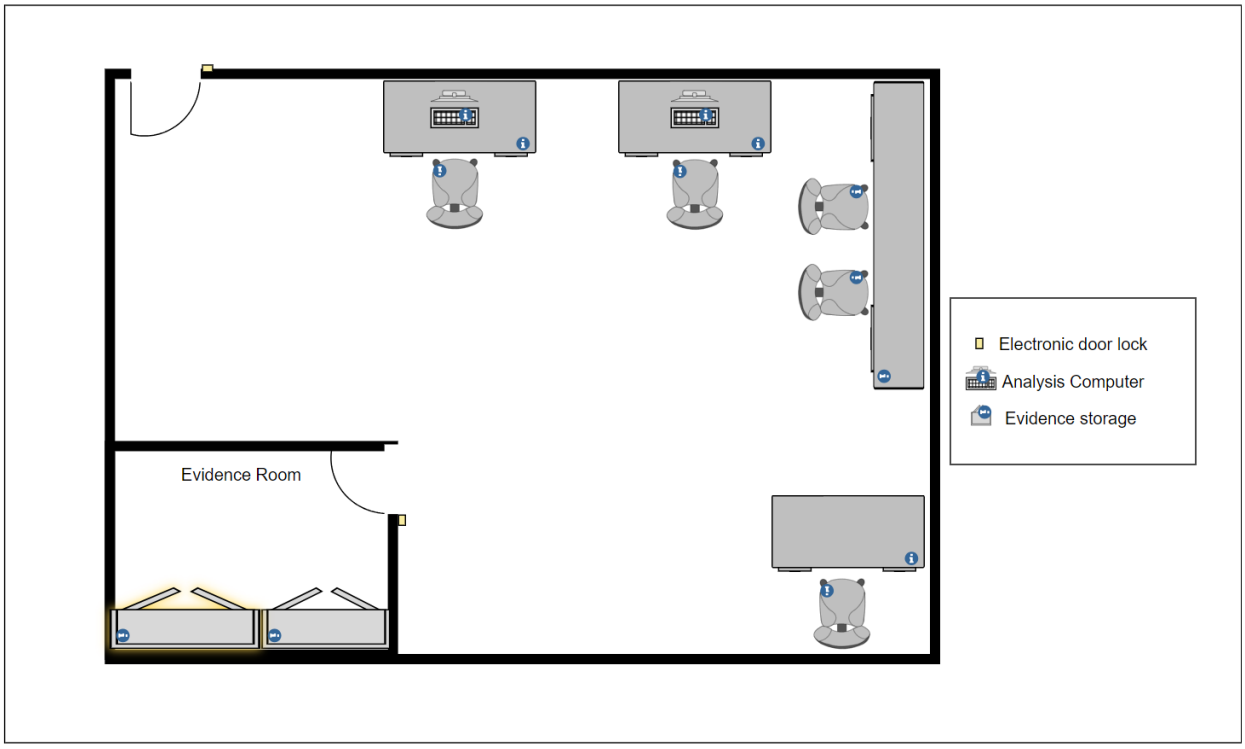
ANSI-ASQ National Accreditation Board (ANAB)
Accredits forensic labs, including digital forensics, based on ISO/IEC 17025:2017 standards.

Forensic Quality Services (FQS)
Provides accreditation for forensic labs focused on digital evidence.

International Accreditation Service (IAS)
Offers accreditation for labs, including those specializing in digital forensics.

(For U.S.-based labs with international ties) United Kingdom Accreditation Service. Although UKAS is based in the UK, they provide accreditation for forensic science laboratories in the U.S. that work with digital forensics.

Forensic Lab Floorplan



Inventory

Hardware

Computers

- Analysis Computers (2)
- Forensic Workstations (2)

Networking Equipment

- Cisco Switch
- Fluke Network Cable Tester
- 15 CAT 6E Cables

Cables and Connectors

- 15 IDE Cables
- 15 SATA Cables
- PC Power Cables

Furniture/peripherals

- Computer Chairs (5)
- Monitors (2)
- Keyboards (2)
- Mice (2)
- Desks (4)

Data Acquisition Tools

- Helix Pro
- Forensic Duplicator

Testing Equipment

- Spectrum Analyzer

Software

Operating Systems

- Kali Linux

Network Analysis Tools

- Wireshark

Forensic Software

- FTK Imager
- EnCase
- X1 Social Discovery

PC Components

- Adapters and other necessary cables

Maintenance Plan

This plan outlines the necessary calibration and upkeep procedures to guarantee the precision and dependability of the lab's equipment and systems. Regular maintenance activities will include:

Scheduled Calibration
All measurement devices and forensic tools will undergo routine calibration according to the manufacturer's specifications to maintain their accuracy.

Preventive Maintenance
A proactive approach will be taken to perform preventive maintenance on all hardware and software components, including cleaning, software updates, and performance checks, to minimize the risk of malfunctions during testing.

Documentation
Detailed records will be kept for all calibration and maintenance activities, including dates, results, and any corrective actions taken, to ensure compliance.

Training
Staff will receive regular training on the proper use and care of equipment to enhance operational efficiency and reduce wear and tear.

Evaluation and Assessment
The maintenance plan will be reviewed annually to assess its effectiveness and make necessary adjustments based on equipment performance and technological advancements.

Staffing positions and Role requirements

Lab Manager – Oversees operations, manages staff, and ensures accreditation.

- Supervise forensic examiners and lab technicians.
- Ensure compliance with ISO/IEC 17025:2017 and other relevant standards.
- Develop and enforce lab policies, protocols, and quality assurance procedures.
- Manage case assignments, monitor progress, and ensure timely completion.
- Oversee the maintenance and calibration of all forensic equipment.
- Handle budgetary oversight, procurement of new tools/software, and manage vendor relationships.
- Conduct audits and ensure that the lab maintains accreditation with appropriate bodies (e.g., ANAB).
- Liaise with law enforcement officials, attorneys, and other relevant agencies regarding case management and lab activities.
- Provide training and professional development for staff.

Digital Forensics Technician – Handles evidence collection, equipment setup, and maintenance.

- Assist in collecting and preserving digital evidence from various devices (computers, mobile phones, storage media).
- Set up forensic workstations and maintain hardware and software tools.
- Ensure proper chain of custody for all digital evidence.
- Perform basic forensic tasks like imaging drives, processing data, and initial triage of evidence.

- Perform routine maintenance on forensic software and hardware.
- Support forensic analysts by preparing equipment and setting up systems for more detailed investigations.
- Assist in documentation, including maintaining logs of evidence intake, processing, and archiving.
- Participate in the lab's quality assurance procedures and assist in preparing for audits.

Forensic Examiner/Analyst – Conducts detailed analysis and investigations of digital evidence.

- Collecting digital evidence from cybercrimes or other types of computer-based crimes
- Extracting data from networks and devices, such as computers, mobile devices, security cameras, drones and Internet of Things (IoT) devices
- Reconstructing the events that led to a cyberattack
- Recovering compromised data
- Restoring data that was damaged or erased from devices
- Identifying vulnerabilities within an organization's cybersecurity infrastructure
- Preparing reports detailing their findings and opinions
- Providing expert witness testimony during court proceedings

Administrative Assistant (optional) – Supports lab staff with documentation and organizational tasks.

Bibliography

(2024, 08 08). Retrieved from Magnet Forensics: https://www.magnetforensics.com/blog/digital-forensics-tools-the-ultimate-guide-2024/

Digital Forensic Examiner: Salary and Job Description. (2024, 10). Retrieved from Augusta University: https://insider.augusta.edu/digital-forensic-examiner-salary/#:~:text=Collecting%20digital%20evidence%20from%20cybercrimes,Recovering%20compromised%20data

ISO/IEC 17025 Forensic Testing Laboratory Accreditation. (n.d.). Retrieved from ANAB : https://anab.ansi.org/accreditation/iso-iec-17025-forensic-testing-laboratory/?srsltid=AfmBOoq3oeK8N6RkBdFQD5y3_uZMSNCYZWoE0HorauAX7SW218LjsQYi

ISO/IEC 17025 General requirements for the competence of testing and calibration laboratories. (2017, 11).