Tristan Woodard

Old Dominion University

CYSE 407

Midterm 1

Cyber Forensics Lab Overview

Summary

ISO/IEC 17025:2017 is the general requirement for the competence of testing and calibration laboratories and is the main ISO standard used by testing and calibration laboratories. ISO/IEC 17025:2017 is the industry standard and has a long track record of success. These standards will be closely adhered to, and accreditation in the standard is to be attained before work can begin.

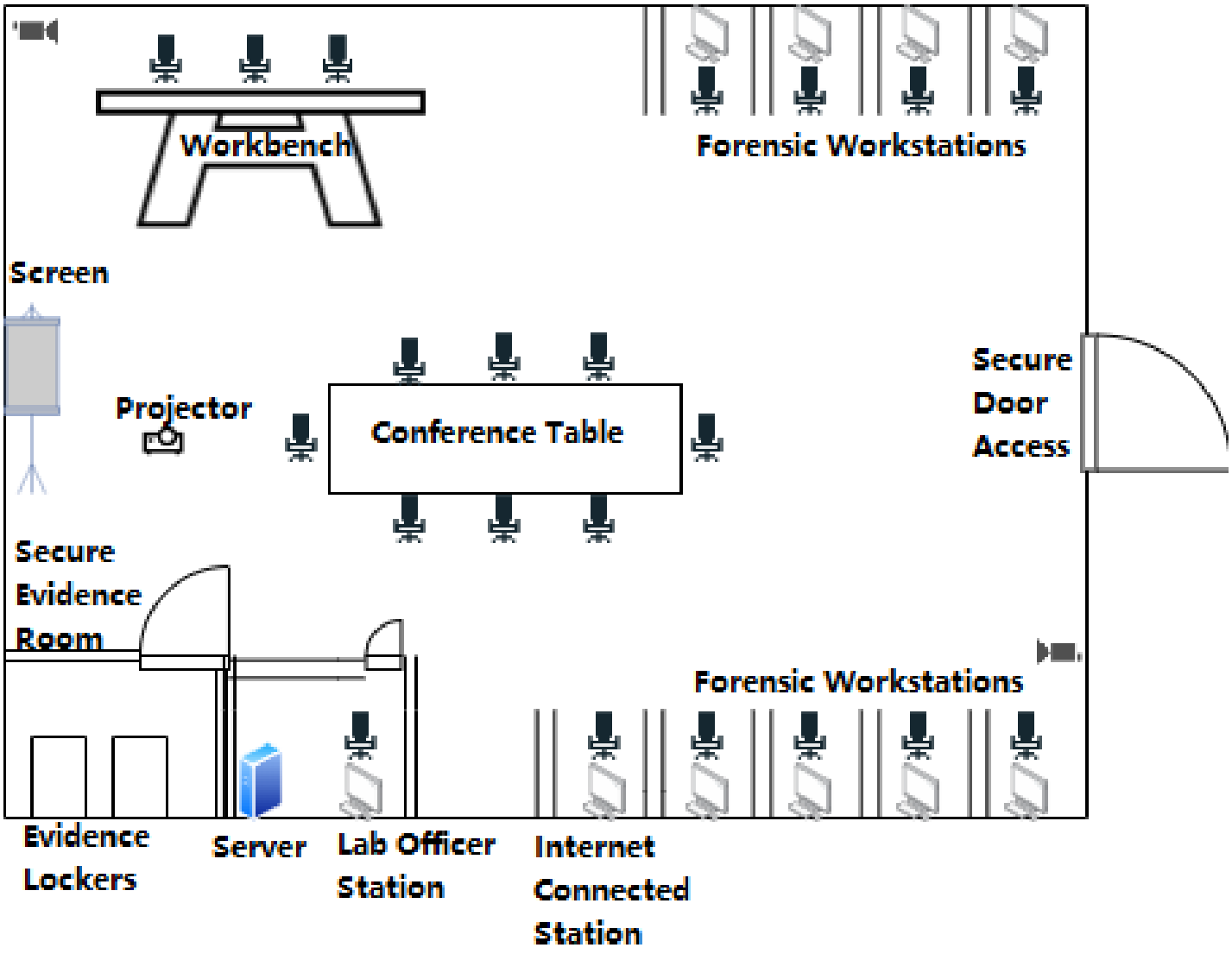
Accreditation Plan

To begin the accreditation process, an accreditation body must be chosen to best suit the needs of the lab. Once the accreditation body is chosen, an application must be sent to the body in order to begin the process of becoming accredited for ISO/IEC 17025:2017.

- The application process should begin promptly, but the accreditation body will ask a variety of in depth questions that could only be answered by a prepared lab and lab staff. The exact questions will depend on the accreditation body and their specific concerns or subjects that need to be addressed. Example questions include: “What is the status of your existing laboratory management system implementation?”, “What is your desired time frame for accreditation?”, and “What is your laboratory's scope of testing and/or calibration?”
- After the initial application process is complete, the accreditation body will present a quote on both the monetary cost and time expected to complete the accreditation process. The lab will in turn accept the quote and enter the contract, or the offer will be declined and the process restarted with another body if there are severe and real concerns concerning the timeframe and price.
- After entering into the contract, the completion of the accreditation process can only end when the lab and lab staff are fully competent in ISO/IEC 17025:2017 and a number of evidential documents are complete and available for the accreditation body. While the accreditation body may require more documentation, required materials include:
    - Staff instruction materials - These detail the specific job responsibilities for each member of staff and how they relate to the upkeep and calibration of equipment.
    - System procedures - Documentation into each of the system components function within the system
    - Quality Manual - Documentation that shows that the lab conforms to ISO/IEC 17025:2017 and how
    - Quality Documents and Records - Various materials that include charts, records, files, and other relevant materials that show how quality will be managed and maintained for contracts
    - Organization Charts and Facilities - Detailed records of the system and lab facilities and organization

    - Internal Audit and Reports - Detail records of internal reports and Audits
- Once the proper materials are prepared and any requested materials are submitted, a series of briefings and meetings will occur between staff and the accreditation body. More materials or revisions may be requested. These will be provided to the accreditation body until assessments are complete
- A final briefing will occur after all assessments are complete. The accreditation body will summarize findings and detail any nonconformities found. The assessment will either be accepted or recommendations will be given on how to fix the nonconformities with corrective action.
- After being accepted for accreditation, the accreditation will be awarded and it will promptly be displayed and maintained.

Laboratory Floor Plan



Inventory

Hardware

Computer Chair x 18
Stationary Chair x3
Desktop x 10

Projector x1
Projector Screen x1
Conference Table x1
Workbench x1
Lab Server x1
Security Camera x2
Evidence Lockers x2
Keyboard x10
Computer Mouse x10
Desktop Screen x10
Network Tester
Spectrum Analyzer
USB Drives
Sata Cables
HDMI Cable
VGA Cable
DVI Cable
RAM Sticks
SATA Cable
HDD Cable
IDE Cable
ATA Plug
Hard Drives
Anti Static Gloves
Anti Static Mats
DVD Writer
Pen Drive
Card Reader

Software

Kali Linux
Wireshark
Helix Pro
Autopsy
COFEE

OSForensics
Windows Server
Microsoft Windows
Microsoft Office Suite
OpenOffice
Write Blocker
Sleuth Kit
Winhex
Oxygen Forensics
EnCase
Access Data Forensic Toolkit
Cellebrite
Anti-Malware
Firewall

Staff Roles/Responsibilities

Lab Manager

- Work to ensure ISO/IEC 17025:2017 compliant procedures are strictly adhered to and followed
- Liaison with law enforcement, accreditation bodies, government bodies, and other outside entities of importance.
- Properly manage devices interacted with
- Perform performance assessment and staff assessment to ensure adherence to duties
- Ensure compliance to other forms of regulations and labor requirements
- Promote and ensure further development of staff skill
- Diffuse workplace conflict
- Procure and implement lab equipment and replacements
- Update policy procedures as required and properly implement updates to entire staff
- Implement proper recruiting procedures to ensure proper staffing
- Train new staff and ensure compliance of new staff to standard

Lab Technician

- Conduct forensic examinations using various pieces of hardware and software
- Assist various other staff and outside partners in ongoing investigations
- Prepare reports and maintain proper documentation and chain of custody documents

- Maintain compliance with ISO/IEC 17025:2017 and other relevant standards and regulations
- Maintain and calibrate equipment as necessary
- Report malfunctioning and miscalibrated equipment as necessary
- Maintain proper communication to staff partners and management to work together to complete investigations

Maintenance Plan

- Maintenance and calibration procedures will be led by the Lab manager and carried out as needed by relevant staff.
- Equipment in need of maintenance beyond day-to-day upkeep will be reported to the lab manager promptly
- The lab manager will implement the notice into the master record of each piece of lab equipment and take note of the necessary need for maintenance or further calibration.
- This master list is to include data like manufacturer, date of issue, identity issued to, software, last calibration and maintenance, and recommended procedure for maintenance and calibration among any other relevant data.
- This list will be updated as necessary and will include all maintenance and repairs with a detailed description of the repair implemented, time, and by whom it was done by.
- Calibration procedures will be documented similarly.
- All calibration, maintenance, and repair procedures will be done as recommended by the master record list kept by the lab manager. The recommended procedures are to be recommended based on the risk, lab requirements, and other empirical data to ensure maximum effectiveness. Unsuccessful or unauthorized repairs or calibrations are to still be noted and reported as possible, even if the full extent is not entirely known.
- Calibration is to occur at a regular interval, with the exact interval required to be kept within the master record list. The lab manager is to ensure this interval will be adhered to. The interval is to be set in order to maintain compliance, promote accurate work, and minimize maintenance needed.
- Preventative maintenance will follow in a manner similar to the previous. Maintenance will be performed at a regular interval as designated by the master record, and will then be thoroughly documented.
- If calibration or maintenance is to be performed by an outside individual or entity, records from the outside organization will be kept within the internal records of the lab.
- If calibration is not required or necessary, intermittent performance and compliance checks will still be carried out and documented at intervals determined by the master record.

- Malfunctioning equipment that fails to meet the standard required for lab compliance and use will be promptly disposed of or sequestered away from the regular work area. It is to be clearly labeled in such a way to ensure it is not to be used, maintained, or disposed of improperly. Disposal plans are to be carried out by the lab manager as soon as possible for the piece of equipment. Replacement equipment is to be acquired as soon as possible.

Bibliography

https://www.iso.org/standard/66912.html

https://17025store.com/step-by-step/

M. M. Parvez, S. A. Hossain and S. M. R. Ali, "Design and implementation of low cost digital forensic laboratory for university," *2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, Chennai, India, 2017, pp. 1524-1528, doi: 10.1109/WiSPNET.2017.8300016.

https://policecareers.tal.net/vx/mobile-0/appcentre-External/brand-3/candidate/so/pm/6/pl/1/opp/5435-Digital-Forensics-Lab-Manager/en-GB

https://www.pjlabs.com/downloads/Steps_17025_Rev%207-09.pdf

https://www.governmentjobs.com/careers/hillsboro/classspecs/862521#:~:text=Conducts%20forensic%20examination%20of%20electronic,other%20digital%20data%20storage%20media.&text=Uses%20software%20and%20hardware%20forensic,for%20further%20investigations%20or%20testing.

https://forensicresources.org/wp-content/uploads/2019/07/Equipment-Calibration-and-Maintenance-12-18-2017.pdf