Digital Forensics Midterm

## Summary

Standards from the ISO/IEC 17025:2017 allows for a detailed array of standards that an organization can follow in order to have a productive, safe and organized digital forensics environment. This standard is key for businesses, especially businesses that have the need for labs and other research facilities. It is important that organizations follow standards that can be followed that uphold the legal integrity and the professional integrity of its business.For a police station, accurate information and detailed information is important in a courtroom,this standard allows for a police station to do this with a guideline to follow.

## Accreditation plan

In order for the lab to achieve accreditation then it has to follow these specific steps:

1. Choosing the ANAB (National accreditation board) Provides the ISO/IEC 17025: 2017 standard that the laboratory will follow.
2. The ANAB has a process for a organization to get the accreditation and that includes:

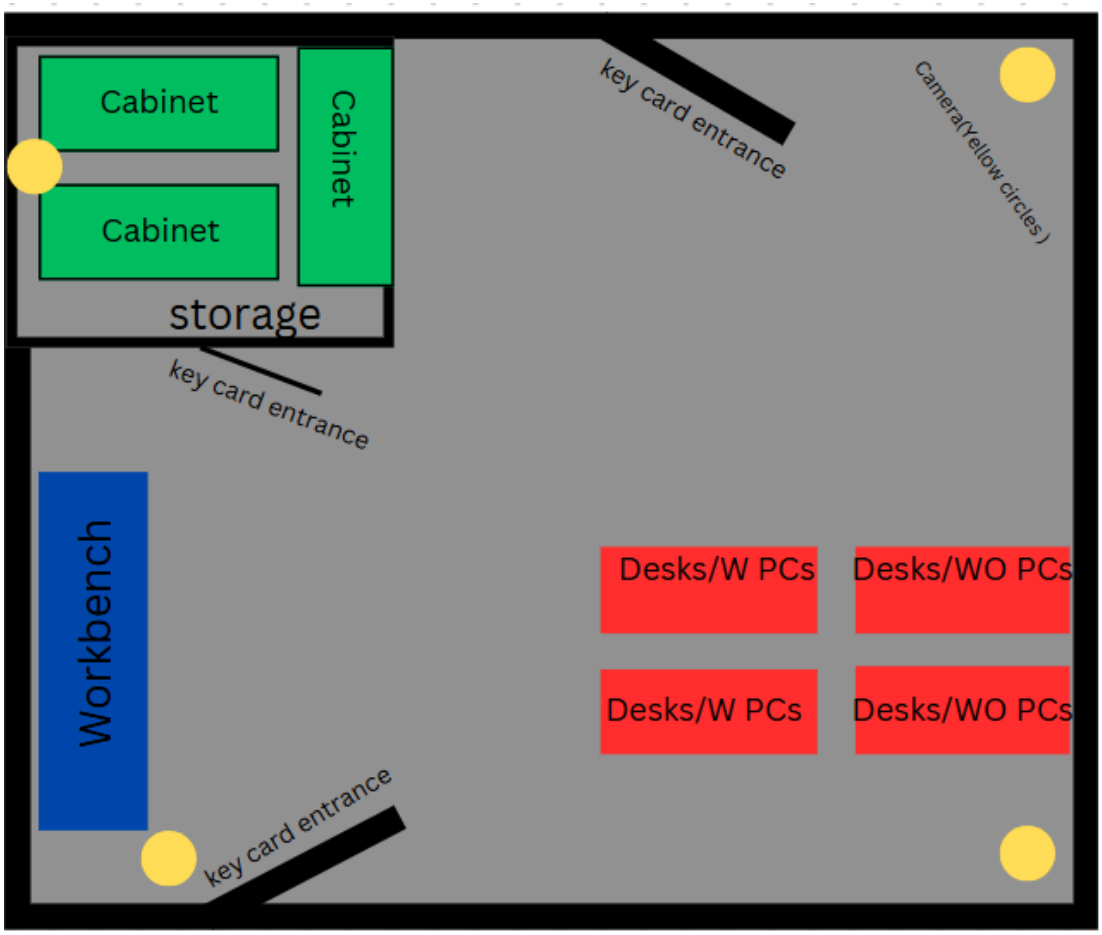
- Receive a quote: Receive a price estimate.
- Apply for the accreditation: submit an application.
- Document gets reviewed:ANAB will review documentation.
- Assessment: ANAB will conduct assessment at the lab site
- Follow-up: Identify any problems within the assessment.
- Decision from accreditation: Receive the decision from ANAB.
- Regular surveillance: Receive periodic surveillance in order to keep accreditation.

With the table below shows a checklist that the laboratory must follow in order to receive and keep ISO/IEC 17025: 2017 accreditation: All requirements must be followed in order for eligibility:

| Policy Topic | Submission Examples | ISO Reference | Required | Initial | Reaccreditation | FoT Addition |
|---|---|---|---|---|---|---|
| ISO/IEC 17205 P | Process of documentation | ISO/IEC 17025:2017 | Yes | | | |
| Site assessment checklist | Fulfilled Checklist | ISO/IEC 17025:2017 | Yes | | | |
| Document control | Logs and documents | ISO/IEC 17025:2017 | Yes | | | |
| Corrective action | Reports | ISO/IEC 17025:2017 | Yes | | | |
| Internal audit | Audited Reports | ISO/IEC 17025:2017 | Yes | | | |
| Management review | Course of action for management review | ISO/IEC 17025:2017 | Yes | | | |
| QA reports | Records for quality assurance | ISO/IEC 17025:2017 | Yes | | | |
| Facilities | Facility blueprints | ISO/IEC 17025:2017 | Yes | | | |
| Test Methods | Test protocols | ISO/IEC 17025:2017 | Yes | | | |
| Traceabilit | Records | ISO/IEC | Yes | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| y | and Logs | 17025:2017 | | | | |
| Uncertainty of Measurement | Measurement data | ISO/IEC 17025:2017 | Yes | | | |

Forensic Lab Floor Plan



## Inventory

### Hardware

- 2 High performance PCs With High Ram
- Multiple Monitors
- Various chargers
- Various charging ports
- Ethernet cables

### Physical Inventory

- 4 Desks
- Chairs
- 3 Evidence cabinets

### Security Inventory

- 4 Cameras
- 3 Keypad access doors
- Safe in storage room for critical backups

### Software Applications

- Wireshark
- Kali
- Windows
- Autopsy
- FTK
- UFS Explorer

## **Staffing**

**Lab manager:**

- Lab manager will be in charge of the overall operation of the lab. This includes making sure that everything and everyone follows the standards of ISO/IEC 17025: 2017. More responsibilities of a Lab manager is to make sure that all lab tools and any lab equipment is safe and ready to use for all technicians that are

on site.Lab manager also is responsible for the budgeting of equipment and establishing training.

**Requirements:**

- Bachelor's degree in computer science, cybersecurity or any related field
- 4+ years of experience in computer science, cybersecurity or any related field
- 2+ years in managing a team in Information systems or digital forensics
- Certifications in one or more of these certifications: Certified Computer Examiner (CCE),Computer Hacking Forensic Investigator (CHFI) and GIAC Certified Forensic Analyst

**Lab Technician:**

- Required to perform analysis that will acquire evidence for any case.Properly use and handle lab equipment under the standards of the laboratory. Understand material that is presented and are able to handle it professionally.

**Requirements:**

- Bachelor's degree in computer science, cybersecurity or any related field
- 2+ years of experience in computer science, cybersecurity or any related field
- Familiar with various Digital forensic software like EnCase, FTK, and Cellebrite.

References:

ANSI National Accreditation Board (ANAB). (2017). *ISO/IEC 17025 forensic calibration*. ANSI National Accreditation Board.https://anab.ansi.org/accreditation/iso-iec-17025-forensic-calibration/

International Accreditation Service. (2021). *ISO/IEC 17025:2017 - International standard for testing and calibration laboratories*. International Accreditation Service. https://www.iasonline.org/wp-content/uploads/2021/02/ISO-IEC-17025-2017-IAS.pdf