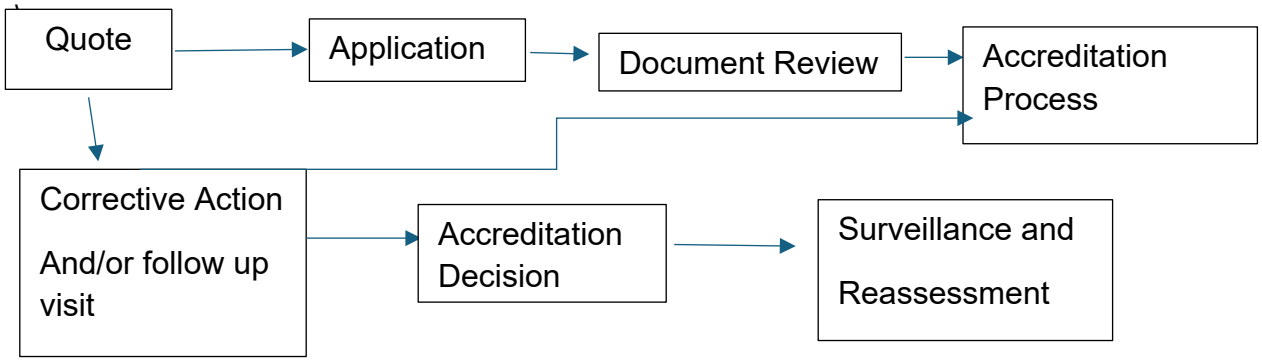
Lilibeth Rodriguez Sanchez

Midterm

Case Scenario: You have been hired to create and run a brand-new digital forensics lab for a mid-sized police department. Your assignment is to come up with a plan for the lab for the next 3 years.

Accreditation Plan: In this lab I will be using the Accreditation plan ISO/IEC 17025 Forensic testing laboratory accreditation. This accreditation plan provides authorization in a lab that has an acceptable quality management system. The plan has the capability and knowledge to provide testing and calibration results.



Step 1: The laboratory is a significance of accreditation, when they are to visit the A2LA. That is the website that will ensure that the correct application forms and documents and the checklist that is to be listed on the website.

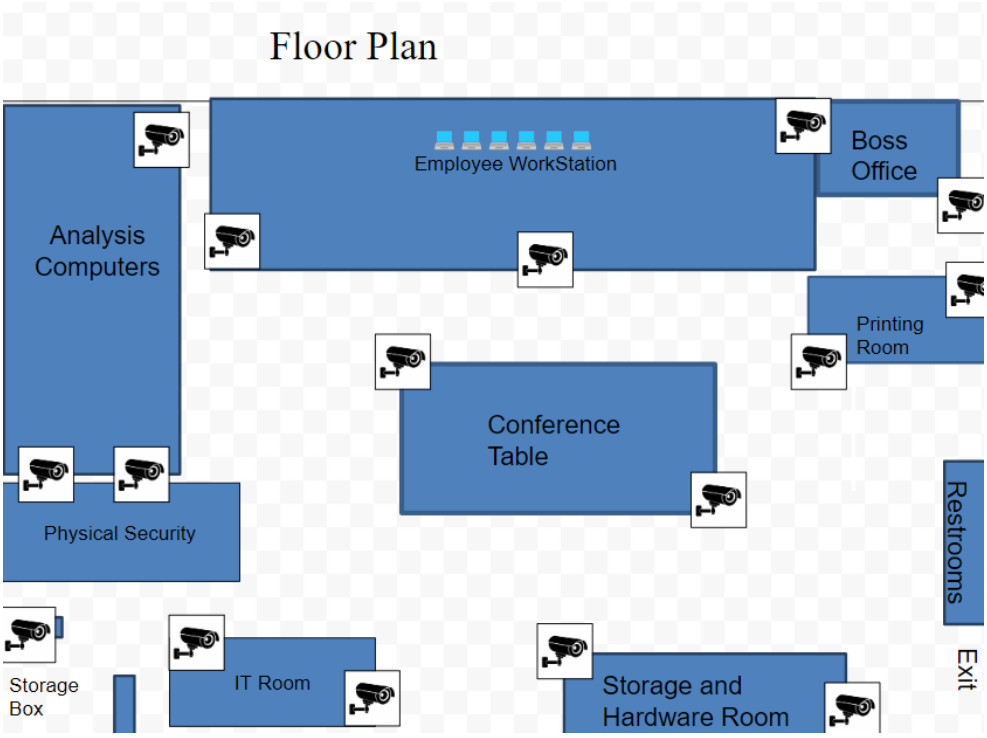
Step 2: Once getting the documentation needed it is important to involve the funding purposes. Government officials must approve before anything can be started.

Step 3: Once the laboratory gets the approval, to start operating it is necessary for a specific location to be concluded in order to work.

Step 4: In the process it is now time to find individuals who are qualified to work in the lab and have the experience necessary to be capable of working in the lab.

Step 5: In the step we find the specified equipment that would be necessary to use in the lab, this equipment must be approved by the A2LA website, in a negotiable price so we avoid overpaying for the equipment.

Step 6: It is now time to set up the laboratory for it to be investigated, Once the documents are submitted, reviewed, and approved by the ISO IEC 17025 accredited by ensuring that any necessary fees were paid for. Then the laboratory can be recognized.



Floor Plan Features:

- In the blueprint above the floor plan involves a conference table, in this conference table meetings and any necessary gatherings will be held.
- The plan has a storage box incorporated to store evidence that is being used for an investigation, and any important files that must be stored.
- In the floor plan there is an IT room that will ensure a spot for any IT issues with hardware and software to be resolved. This room will ensure a zone to be able to mitigate the issues.
- With any floor plan, restrooms are necessary and are available whenever employees are in need.
- In the display I incorporated a hardware and software room that allows for the display of any extra inventory that is not being used currently in the laboratory
- I also included physical security in the floor plan in order to have employees scan their ID before entering the building due to it being crucial for me for them to be a security guard present.
- I included a printing room to have a specific section in which employees can print out anything that is needed.

- In the floor plan there is an employee workstation included in which employees can be able to work on their investigations, the boss's office is located right next to the employee station for the boss to be able to monitor them and provide assistance when needed.
- There is a computer analysis station in which employees can work on
- Throughout the floor plan I incorporated many security cameras to have all employees monitored to make sure that any information is not being distributed to the outside world.

The list below incorporates the hardware that will be accessible to the employees:

- Ram
- Speakers
- Fire Wire
- CPU dual core
- 30 Large Monitors
- 10 printers
- Tape dives
- Tool kit
- Static bag
- Keyboards, mouse, scanner, etc.
- USB
- Hard disk drives
- Mulptiple core processor
- Cables
- Cameras
- First Aid Kit
- Laptop Computers
- Evidence preservation device
- Pen Drives

The list below incorporates the software that will be used by the employees

- Wireshark
- Media Indexing Tool
- Forensic Disk Imaging Tool
- Mobile Field Kit
- Data recovery and restoration tool
- Password recovery tool
- Decryption tool
- Programming languages

- Open-source file viewers
- Antivirus program

The following list incorporates the operating systems that will be used;

- Windows 11
- Linux
- Lamp

Maintenance Plan:

- Regarding the Maintenance Plan, it is crucial for a fire drill to be performed every six months to secure a plan in case of an emergency employees know how to evacuate the building and understand that this alerts them that there is a fire.
- It is important to ensure that no storage file is being altered therefore every week there will be certain employees who will need to check the storage files to make sure everything is fine.
- To ensure security, the door access will be reset every 5 months and therefore will be new keys and will all be given to the employees once reset. This will help if there ever to be an investigation the last employee can be tracked.
- There will be an electrical team every 3 months to make sure that there is enough electrical power to operate the activities necessary
- Plumbing will be taking place every so often to ensure that restrooms are well maintained.
- Security cameras must be well maintained and always operating to ensure recording of all incidents in the organization.

Lab Maintenance Plan:

- For the lab to be well maintained there will be an often updates on the forensic software tools
- Monthly updates on case management systems are necessary to track the progress being made
- There should always be an incident response team that will always be in the lab
- Strict physical access control will be implemented in the lab
- An IT team will be available so that they can check everyone’s working environments, working on computers to make sure that there is no malware or ransomware attack.
- Employees will also practice cyber hygiene, in which they will reset their passwords every single month to ensure safeguarding sensitive information.

Staffing

- Physical Security
- Internal Auditors
- Computer Forensic Experts
- Team leaders

Team Leader Role:

The team leader is responsible for ensuring that their investigations are performed with expert forensic skills. The demonstrate the leadership that other employees should follow. They focus on one area that they have expert skills in and manage the recovery, preservation, and analysis data as well as writing an extensive report outlying all the results.

Qualifications:

- Must have Citizenship
- Bachelor's degree in either computer forensics, IT related field
- Top Security Clearence
- Senior level experience 7 years at least

Must also have any of the following certifications:

- IACIS
- CFCE
- ENCE
- CDFEE

Computer Forensics Expert:

Role: For this role professionals are challenged by getting put into situations that involve issues of organized crime such as hacking, spoofing, social engineering, or terrorism. Their main responsibility is to gather data and evidence that can be crucial for an investigation and analyze it with their expertise.

Qualifications:

- Bachelor's degree in computer forensics or IT related field
- Networking skills
- Problem solving skills
- 1 or more years of experience
- Up to date on forensic tools

Certifications that are preferred:

- CCE
- CISSP
- CompTIA A+

Internal Auditor:

Role: What auditors do, is examine and investigate company record, financial documents, in which they identify compliance concerns risk and fraud, and inaccurate data.

Qualifications:

- Bachelor's degree preferably in business
- Skills in risk management -Managing projects skills
- IT skills
- Systematic skills
- Communicating skills

Certifications preferred:

- CIA
- CPA
- CRMA

Physical Security Officer:

Role: The physical security officers' job is to make sure that nobody should be accessing the lab if they do not have access, or break into it, the way in which they prevent this issue, is from surveillance systems and detection devices, while following lab guideline.

Qualifications:

- Have Citizenship
- Be at least 21 years of age
- Withhold a clean record with no previous criminal activity or felonies
- Have experience in a security area
- Have an associate's degree

Certifications are not required for this position.

Bibliography:

8 physical security certifications to enhance your knowledge - indeed. (n.d.-a). https://www.indeed.com/career-advice/career-development/physical-security-certifications-list

A2la.qualtraxcloud.com. (n.d.-b). https://a2la.qualtraxcloud.com/ShowDocument.aspx?ID=567

Building a BASIC computer forensics laboratory. (n.d.-c). https://www.oas.org/juridico/spanish/cyber/cyb32_forensics_lab_en.pd

Calibration laboratory accreditation program. A2LA. (2023, April 5). https://a2la.org/accreditation/calibration

Carpenter, J. W. (n.d.). Internal Auditor: Career path and qualifications. Investopedia. https://www.investopedia.com/articles/professionals/120115/internal-auditor-career-path-qualifications.asp#:~:text=in%20the%20organization.-,Educational%20Qualifications,administration%20or%20computer%20information%20systems.

Digital Forensic Analyst Team lead. Cybervance. (2020, June 1). https://cybervance.com/job/washington-d-c-full-time-digital-forensic-analyst-team-lead/

Forensic laboratories: Handbook for Facility Planning, Design ... (n.d.-d). https://www.ojp.gov/pdffiles/168106.pdf

Forensicsware. (n.d.-a). Home. Cyber Lab Setup Digital Forensic Lab Experts for Hardware, Software & Training. https://www.forensicsware.com/lab-setup.html

Forensicsware. (n.d.-b). Home. Cyber Lab Setup Digital Forensic Lab Experts for Hardware,

Software & Training. https://www.forensicsware.com/lab-setup.html

The Investigation Team and their roles: The important role of Investigation Team. Financial Crime Academy. (2023, November 27). https://financialcrimeacademy.org/the-investigation-team-and-their-roles/

Pro-nt-124. Transition plan for the implementation of ISO/IEC 17025:2017, related to CBs accredited by ANSI National Accreditation Board as product certification bodies. (n.d.). https://anabpd.ansi.org/accreditation/product-certification/DocumentDetail?DRId=20879&PId=1#

Sampling for testing. A2LA. (2022, November 9). https://a2la.org/accreditation/sampling

Stages and resources for standards development. ISO. (2019, May 20). https://www.iso.org/stages-and-resources-for-standards-development.html

What does an internal auditor do?. Accounting.com. (2023, October 24). https://www.accounting.com/careers/internal-auditor/#:~:text=Internal%20auditors%20examine%20and%20analyze,%2C%20fraud%2C%20and%20data%20inaccuracies.

What is a computer forensics analyst?: Skills and career paths. Explore Cybersecurity Degrees and Careers | CyberDegrees.org. (2022, December 8). https://www.cyberdegrees.org/jobs/computer-forensics/#:~:text=Computer%20forensics%20analysts%20assist%20in,expert%20insights%20during%20court%20proceedings.

What is ISO 17025 accreditation? why are ISO 17025 accredited calibrations important?. What is ISO 17025 Accreditation?: Why are ISO 17025 accredited... (n.d.). https://www.campbellsci.ca/why-is-iso17025-calibration-important#:~:text=ISO%2017025%20Accreditation%20proves%20a,provide%20testing%20and%20calibration%20results.