Summary

Outlining a plan for a mid-sized Police agency's computer forensic lab may first require a detailed review of the regulations and standards that are applicable to the location, state or country to which one wanted to build the forensic lab on. Because conducting investigation and storing evidence should meet the accreditation requirement of the state or the country. In the US and internationally, ANAB-ASQ is one of the well-known forensic lab accreditation bodies, which makes sure that correct and consistent results are produced through rigorous audit of the task and procedures.

To check the plan outline, ANAB-ASQ can provide the ISO/IEC 17025 standard for the plan. Mid-sized police department lab plan may additionally consider using the most diverse, legacy software and hardware systems or digital investigation specifically because the communities it serves will usually use a wide verities of computing systems. Alternative lists of approved accreditation organizations in the US are provided at the bottom of this page.

Having the budget plan which lists how much this police department is willing to spend to build the new lab-station with a larger emphasis on what it will cost to recurrently maintain and stay updated with the rapidly growing technological advances is also important.

Accreditation Plan

1. According to ANSI-national accreditation board information (ANAB) website, the steps to standardize a computer forensic lab on the ISO/IEC 17025 will require the computer forensic lab owner's demonstration of its competencies to execute and perform works, effectiveness of its management systems and readiness in respecting the rules in place and conform to all the written regulation in the program to which it is applying. The computer forensic lab, the police department in our case, should also demonstrate that the forensic and testing services will ensure the accuracy, reliability and impartiality of the process that must be performed in a lab appropriate environment (facility, equipment and method). The skills, experiences and qualifications of its personals and workforce are also checked and verified.
    a. A quality manual, outlining the policies and procedures that ensure the accuracy, reliability and impartiality of its calibration services is needed to be included during application. The police department unit's structure that is handling this lab roles and responsibilities also needs to be clearly described.
    b. The police lab unit should show that its personnel possess the latest training and experience necessary to meet the needs of the current forensic testing and calibration services.
    c. The quality of the methods and equipment the police department is setting up to use are to be confirmed valid and proficient to execute the necessary tasks.
    d. The police department must demonstrate that it will protect the confidentiality and integrity of people's information that is consistent with the chain of custody.
2. **List of Approved Accreditation Organizations in the US:**
    a. ANSI National Accreditation Board (ANAB)

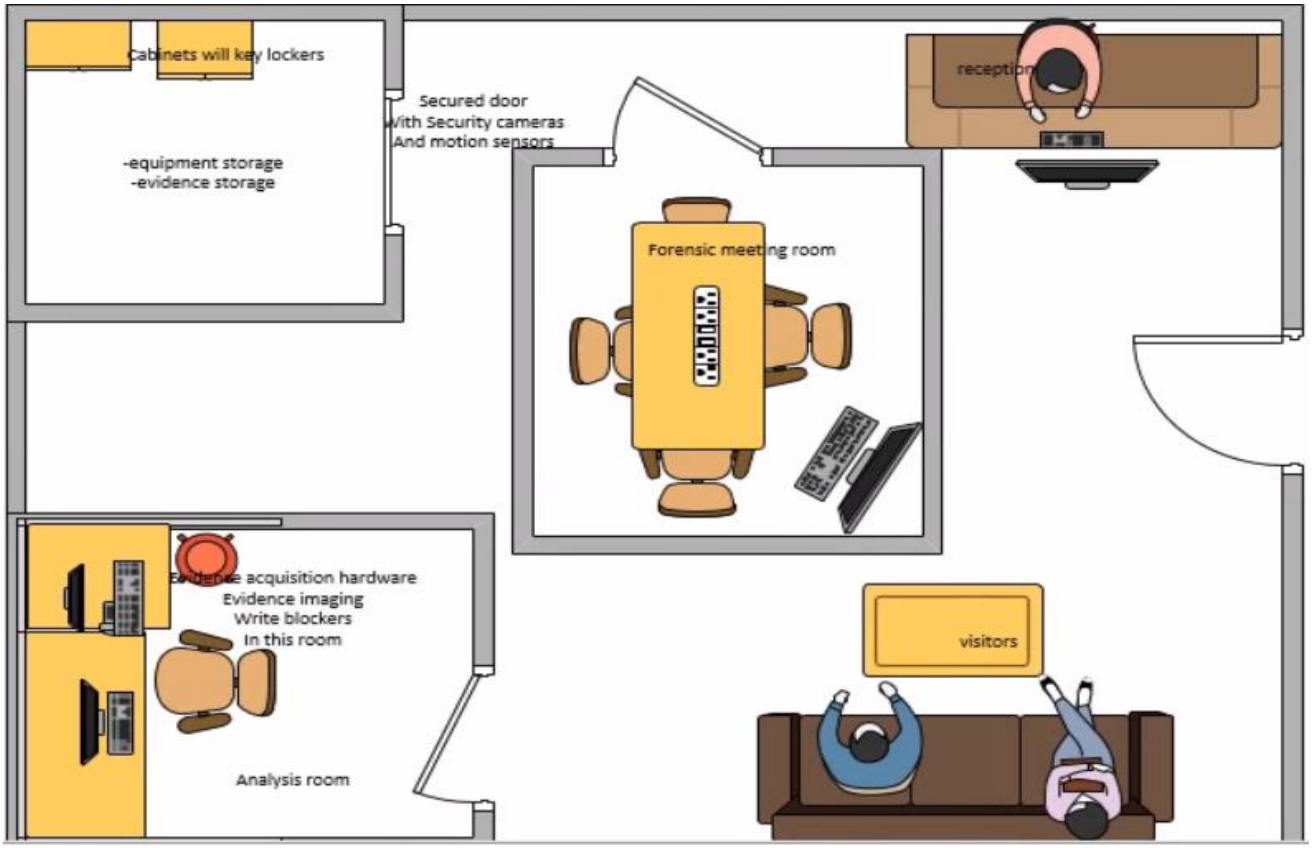
b. American Society of Crime Laboratory Directors/Laboratory Accreditation Board (ASCLD/LAB)
c. National Institute of Standards and Technology (NIST)
d. International Organization for Standardization (ISO)
e. Accredited Standards Committee X9, Inc. (ASC X9)

3. Some items than are included in the ISO/IEC 17205 accreditation application check list of a med-size computer forensic lab can be

Checklist Items for accreditation	Description of
1. Quality management system documentation	Includes policies, procedures, and work instructions for managing laboratory operations and maintaining the quality of forensic services
2. Organizational structure and personnel qualifications	Includes information on the qualifications and experience of laboratory personnel, including resumes, training records, and job descriptions
3. Equipment and calibration records	Includes information on the equipment used in forensic analysis, including calibration and maintenance records
4. Sample handling procedures and documentation	Includes policies and procedures for handling, transporting, and storing digital evidence, as well as documentation of chain of custody and traceability
5. Method validation procedures and documentation	Includes procedures for validating forensic methods, such as software analysis tools, and documentation of validation studies
6. Records of measurement uncertainty and error	Includes records of measurement uncertainty and error for each measurement or test result, which is important for assessing the reliability and accuracy of forensic analysis
7. Internal audit procedures and documentation	Includes procedures for internal audits of laboratory operations and documentation of audit reports and follow-up actions
8. Corrective action procedures and documentation	Includes procedures for corrective actions to address nonconformities or areas for improvement, and documentation of nonconformance reports and follow-up actions
9. Preventive action procedures and documentation	Includes procedures for preventive actions to address nonconformities or areas for improvement, and documentation of

	nonconformance reports and follow-up actions
10. Proficiency testing and inter-laboratory comparison results	Includes records of proficiency testing and inter-laboratory comparison results, which are important for demonstrating the competence of the laboratory and the accuracy of forensic analysis
11. Records of customer complaints and their resolution	Includes records of customer complaints and their resolution, which is important for addressing any issues and improving customer satisfaction
12. Management review and continuous improvement processes	Includes procedures for management review of laboratory operations and performance, and documentation of action plans for continuous improvement

Forensic Laboratory floor plan (created using Visio)



Inventory

Hardware	Software
• Computer desktop for forensic lab • Laptop for remote or onsite investigation • Storage devices • Write blocker tools • Forensic imaging tools • Network, switch, cables and adopters • Video and audio recording equipment • Environmental controlling equipment (humidity sensors and air filters) • Security equipment (security cameras, motion sensors and access control systems) • Evidence collecting tools	• All versions of Microsoft offices • Hexadecimal Editors • Kali Linux • Programming languages, such as Python, Ruby, or Visual Studio • Specialized image viewers • WPS office and WordPerfect • EnCase, FTK, or Autopsy • Wireshark or Network Miner • John the Ripper or Hash-Cat • management software for managing case-related files and notes, such as Microsoft OneNote or Evernote.
Other necessities • Office accessories, chairs and workstation**.** • Computer hand tools, such as Phillips and flathead screwdrivers, a socket wrench, any vendor-specific tools, a small flashlight, and an antistatic wrist strap • Chain of custody forms and related documentation • Protective equipment for lab personnel, such as gloves, lab coats, and face masks • Calibration equipment and reference standards for maintaining accuracy and precision of lab equipment • Cleaning supplies for maintaining a clean and sterile lab environment	

Maintenance Plan

The essentiality of the maintenance needs for this computer forensic lab is to ensure that the software and hardware inventories are at their best to produce valid and accurate lab results. Some list of plans that may be useful for the police departments can be:

- software and operating systems should maintain the latest compatible licensed copies of the legacy OSs and software. Scheduling updates of operating systems, software, and drivers must ensure that all systems are up to date and secure.
- Software and hardware inventory should include current and older versions.
- Regular cleaning of hardware components such as keyboards, mice, monitors, and computer cases to prevent dust buildup and overheating.
- Installation of anti-virus and anti-malware software to prevent and detect any potential threats or malicious code.
- Regular backups of data and system images to prevent loss of data in the event of a hardware failure or system crash.
- Periodic testing of hardware components such as hard drives, memory, and power supplies to detect any potential issues and replace them before they fail.
- Implementation of a secure data destruction plan to ensure that all data on retired hardware is securely erased.
- Regular training and awareness programs for lab personnel to ensure they are aware of the latest threats and techniques in digital forensics.
- Implementation of access controls and logging to ensure that all lab activities are tracked and auditable.
- Periodic testing of the lab's procedures and protocols to ensure they are effective and compliant with all relevant standards and regulations.
- Regular reviews of the lab's equipment and software inventory to ensure that all items are properly licensed and maintained.
- Physical access doors and entries functionality are to be checked regularly.

Roles and Responsibilities of Lab Manager and technical staff

Manager:

- The lab manager is responsible for setting up processes and enforcing ethical standards.
- Supervise and manage the lab staff, including technical staff and other support staff.
- Ensure the quality of work in the lab and maintain a high level of professionalism and ethical standards.
- Introduce necessary policies, procedures, and work instructions for management of laboratory operations
- Maintaining fiscal responsibility for lab's budget, resources, and equipment.
- Manages plans and updates for the lab, such as new hardware and software purchases, so that the latest developments in computer forensics and related technics are introduced.
- Develop and implement lab policies and procedures to ensure efficient and effective operations.

- Establishes and promotes quality assurance processes for the lab's staff to follow, such as outlining what to do when a case arrives, logging evidence, specifying who can enter the lab, and establishing guidelines for filing reports. To ensure the lab's efficiency, the lab manager also sets reasonable production schedules for processing work.
- Coordinate with law enforcement agencies, attorneys, and other stakeholders in the investigation and prosecution of criminal cases.

Technical staff

- Staff members in the forensics lab should have enough training to perform their tasks. Necessary skills include hardware and software knowledge, including OSs and file types, and deductive reasoning**.**
- Conduct digital forensics examinations on computers and other electronic devices related to criminal investigations.
- Perform data recovery, analysis, and preservation of electronic evidence in accordance with established protocols and procedures.
- Staff members are also responsible for continuing technical training to update their investigative and computer skills and maintaining a record of the training they have completed
- Maintain the integrity of evidence and chain of custody throughout the forensic process.
- Document and report findings and conclusions to law enforcement agencies, attorneys, and other stakeholders.
- Testify in court as an expert witness on digital forensics issues.
- Assist in the development and implementation of lab policies and procedures.

Reference:

Mainly our textbook "guide to computer forensic and investigation" was used as a reference for this assignment. Materials searched online like the ANAB websites are also used to enrich the resources on our book. Visio accessed through ODU-VM were used to floor plan and screen shot is submitted.