CYSE 406 Midterm

Summary

Article I. Lab Accreditation

To begin an accreditation for a digital forensic lab for International Standard ISO/IEC 17025:2005 a lab must apply for "General Requirements for the Competence of Testing and Calibration Laboratories" and provide evidence of ownership of this document prior to applying for accreditation. This plan will use the ANB and ISO 17025:2005 standards for accreditation. The following steps will be used to start the accreditation process:

1. The application process will take place for accreditation with the ANAB. This application process will ensure that the lab is complying with all ISO/IEC 17025 requirements. The accreditation process will include the following steps.
    a. Quotation
    b. Application
    c. Document Review
    d. On-Site Assessment
    e. Resolution of Non-Conformities
    f. Accreditation Decision
    g. Conformance Monitoring and reassessment every 4 years

2. Documentation of the following will be provided to assist during the accreditation process. (Information obtained from https://www.justice.gov/archives/ncfs/file/839701/download)
    a. Written Procedures for evidence including security and handling
    b. Written reports for all examinations
    c. Review process of examinations
    d. Procedures for interviews and monitoring of interviews
    e. Proper note taking procedures of all investigations
    f. Technical procedures
    g. Training and certification programs and continued education programs to ensure employees are trained regularly with all current standards.
    h. Proficiency testing
    i. Corrective and preventive action processes

3. Completion of the site assessment checklists and submission

4. List of Approved Accreditation Organizations in the US:
    a. FEPAC: Forensic Science Education Accreditation Commission (https://www.aafs.org/FEPAC)

b. A2AL: Forensic Examination Accreditation Program (https://a2la.org/accreditation/forensics/)
c. The ANSI-ASQ National Accreditation Board and their recent acquisitions of L-A-B and ASCLD-LAB which are now both (http://www.anab.org/) ANAB
d. GIAC: Global Information Assurance Certification (https://www.giac.org/focus-areas/digital-forensics-incident-response/)

5. Fees: Contact the ANSI-ASQ National Accreditation Board (ANAB) website for information on accreditation fees at http://www.anab.org/lab-related-accreditation/request-for-quote

6. The laboratory must be familiar with and comply with all relevant ISO/IEC 17025:2005. The table below serves as a sample for the ISO checklist for an accreditation application. The necessary steps for accreditation are listed:

Policy Topic	**Attachment Number**	**Submissions Examples Required**	Initial
4.2 Confidentiality	4.2.4 ISO/IEC 17025:2017	Do personnel, including any committee members, contractors, personnel of external bodies, or individuals acting on the laboratory's behalf, keep confidential all information obtained or created during the performance of laboratory activities, except as required by law?	
5. Structural requirements	5.2 ISO/IEC 17025:2017	Does the laboratory identify management that has overall responsibility for the laboratory?	
6.1 General	5.7 ISO/IEC 17025:2017	Does the laboratory have available the personnel, facilities, equipment, systems and support services necessary to manage and perform its laboratory activities?	
6.2 Personnel	6.2.3 ISO/IEC 17025:2017	Does the laboratory ensure that the personnel have the competence to perform laboratory activities for which they are responsible and to evaluate the significance of deviations?	
6.2 Personnel	6.2.2 ISO/IEC 17025:2017	Does the laboratory document the competence requirements for each function influencing the results of laboratory activities, including requirements for education, qualification, training, technical knowledge, skills and experience?	
6.3 Facilities and environmental conditions	6.3.3 ISO/IEC 17025:2017	Does the laboratory monitor, control, and record environmental conditions in accordance with relevant specifications, methods, or procedures or where they influence the validity of the results?	

6.3 Facilities and environmental conditions	6.3.4.1 ANAB Accreditation Requirement	Is there a procedure that addresses security and access to areas where testing and calibration occur?	
6.4 Equipment	6.4.3 ISO/IEC 17025:2017	Does the laboratory have a procedure for handling, transport, storage, use, and planned maintenance of equipment in order to ensure proper functioning and to prevent contamination or deterioration?	
6.4 Equipment	6.4.9 ISO/IEC 17025:2017	Is equipment that has been subjected to overloading or mishandling, gives questionable results, or has been shown to be defective or outside specified requirements, taken out of service? Is it isolated to prevent its use or clearly labelled or marked as being out of service until it has been verified to perform correctly? Does the laboratory examine the effect of the defect or deviation from specified requirements and initiate the management of nonconforming work procedure (see 7.10)?	
6.4 Equipment	6.4.12 ISO/IEC 17025:2017	Does the laboratory take practicable measures to prevent unintended adjustments of equipment from invalidating results?	
7.5 Technical records	7.5.1 ISO/IEC 17025:2017	Does the laboratory ensure that technical records for each laboratory activity contain the results, report, and sufficient information to facilitate, if possible, identification of factors affecting the measurement result and its associated measurement uncertainty and enable the repetition of the laboratory activity under conditions as close as possible to the original? Do the technical records include the date and the identity of personnel responsible for each laboratory activity and for checking data and results? Are original observations, data, and calculations recorded at the time they are made and identifiable with the specific task?	
7.5 Technical records	7.5.1.4 ANAB Accreditation Requirement	Are records created or maintained in a permanent manner?	
7.7 Ensuring the validity of results	7.7.2 ISO/IEC 17025:2017	Does the laboratory monitor its performance by comparison with results of other laboratories, where available and appropriate? Is the monitoring planned and reviewed and include, but not be limited to, either or both of the following: a) participation in proficiency testing or NOTE ISO/IEC 17043 contains additional information on proficiency tests and proficiency testing providers. Proficiency testing providers that meet the requirements of ISO/IEC 17043 are considered to be competent.	

		b) participation in interlaboratory comparisons other than proficiency testing?	

Sample Checklist Items obtained from Section Internal Audit Checklist North Carolina State Crime Laboratory

Article II. Lab Maintenance Plan

1. **Scope –** These practices apply to casework units of the forensic science lab with instrumentation and equipment that influence the validity of forensic examinations.
2. **Roles –**
    a. **Lab Manager – (1 position to be filled)** 5+ years of relevant experience at an intermediate to expert level in forensic investigation. Bachelors degree in either forensic science or computer science required. Iso standards certification shall be obtained withing 12 months of starting, previous certification preferred.
        i. **Job Description**
            1. Conduct budget reports for lab resources
            2. Ensure Staff members are trained to current standards
            3. Hold team up to ethical expectation
            4. Promote quality assurance processes
            5. Equally distribute cases among staff
            6. Respond to crime scenes and collect evidence including photographic and digital evidence.
            7. Ensure all equipment is maintained properly
            8. Provide staff with all needed resources including coaching
            9. Perform corrective action when needed
            10. Prepare team and lab for Audits
            11. Ensure all regulations are met including health and safety
            12. Continually review changes to standards and execute the changes needed in the lab. (Keep up to data with ISO 17025)
            13. Experience using several forensic pro
    b. **Digital Forensic Technician – (2 positions to be filled)**
        i. A 4-year BS or BA degree in the preferred concentrations: Computer Science, Engineering, Information Technology, or Management of Information Systems.
            1. Conduct investigations in a timely and productive manor
            2. Ability to follow all procedures and standards including crime scene processing, transportation and collection of evidence, examination of evidence

3. Produce clear accurate reports of investigation findings
4. Perform all activities in a safe manor
5. Follow all procedures as set by the lab manager
6. Continue training and maintain certifications where needed
7. Technical quality checks
8. Wide array of investigative knowledge of multiple Oss and devices (Phone, computers, flash drives, Tablets, video game consoles etc)
9. Conduct investigations in an ethical manor

3. **Maintenance Practices –** In order to keep the lab maintained, regular cleaning, repairs, and calibrations of equipment will be performed to the specifications set forth by the manufacturer. Records of maintenance will be kept in timely intervals to ensure that equipment produces accurate results with consistency.
    a. Logs will include the equipment model, manufacture (and support contact information) , calibration test results as well as cleaning procedures. Signature of lab technician performing these practices must be recorded.
    b. Operating systems will be kept up to date at a semi-annual channel and all urgent patches will be made in an appropriate timeframe to ensure security of devices. This will be done in a configuration management log
    c. Daily interval back ups of workstations and monthly full back ups of analysis workstations
4. **Calibration Procedures –** The Calibration of equipment is essential to maintain accurate and consistent results. This is used to minimize uncertainty in results. All calibration of equipment will be performed to manufacture recommendations to ensure the lab equipment performs as intended. These procedures will be fully documented and performed at manufacturer recommended intervals.
5. **Calibration Interval –** Calibration of equipment will be performed by Technicians and manager. Calibration of all equipment will be performed on a regularly scheduled basis according to manufacturer guidelines. Results during each interval will be recorded and compared with previous calibration reports to ensure accuracy of the results.
6. **Maintenance –** All equipment will be properly maintained at all times. This includes regular cleaning of equipment and proper storage of equipment. All evidence susceptible to damage from static electricity will be stored in antistatic bags. Maintenance of electronic devices will be done with proper safeguards such as use of antistatic wrist straps and anti-static mats. Components on analysis workstations will be regularly updated including drivers. Operating systems will be regularly patched. Regular back ups of systems will be taken and stored locally on our RAID server. (See hardware section) The laboratory manager will ensure that technicians service all workstations and devices according to manufacturer intervals and specifications, this includes calibration. Where a technician is unavailable to perform these duties, it will be the responsibility of the lab manager. Cleaning staff will have access to main laboratory, however the evidence room will be maintained and cleaned only by those with proper clearance. Beverage consumption by staff will be allowed in lab, only at the technician's workstation, a lid will be required on all beverage containers. Food consumption in lab prohibited to ensure equipment safety.

7. **Preventative Maintenance –** Replacement of forensics equipment will be done every 24 to 36 months or per manufacturer warranty expiration. Workstations will be replaced ever 36 months. Any components that are subjected to wear will either be replaced by the manufacturer or technician on a case-by-case basis.
8. **Corrective Maintenance –** When equipment is not performing to standards, the issues will be identified and all troubleshooting procedures per manufacturers manual will occur. After the repair has been made, test will be performed and recorded. The test will be compared to the most recent Calibration intervals to assure the equipment is operating at its intended standards. Where applicable, service will be performed by the manufacturer.
9. **Performance checks –** Where calibration is not required performance checks will be regularly performed to ensure the consistent and accurate results of all equipment and workstations. Routine function checks will take place and performed by technicians in the lab where applicable. Performance checks will be recorded, and maintenance will be performed as needed.
10. **Malfunctioning Equipment** – Any equipment that is malfunctioning or can not be repaired will be replaced either under manufacture warranty or with the most cost-effective measure. If the replacement of a component is more feasible, the replacement will be made and recorded by the repairing technician. If the equipment must be replaced, the old equipment will be disposed of in a secure manor. Equipment replacement, both expected and unexpected will be set in the budget.
11. **Equipment Security** – Equipment will be always secure both physically and over the network where applicable. Firewalls and managed switch will be implemented. Cleaning staff will not have access to workstations. Door Locks will assist with the physical security of the equipment. Cameras are integrated in keypads to support this standard. True floor to ceiling walls will be required fully around the lab as well. Component cabinets will be secured with locks. Evidence room will have access specifically to those authorized and logs will be recorded and audited of access.

Article III. Equipment needs

Office Equipment

5 Desk Chairs

3 heavy duty storage cabinets (3 padlocks for cabinets, key or combinations)

1 Storage cabinet with built in lock (evidence room)

1 Metal shelf for (evidence room)

1 Server Rack

3 workstation desk (Minimum 4’ length)

3 Work Benches (6’ minimum length)

2 Keypads with camera (1 for lab entrance, 1 for evidence room)

2 waste bins

1 paper shredder

Standard office supplies (Pens, printer paper, folders, Permanent markers ETC)

Hardware

3 Monitors (at least 32”) for workstations

2 Workstation PCs (Specs i9 processor, 32gm ram, 8 gb graphics cards and 1TB HHD) (Atleast 1 station Dual boot for windows and Linux OS)

1 Mac Desktop Unit (Specs i9 processor, 32gm ram, 8 gb graphics cards and 1TB HHD)

3 Wired Keyboards and Mice

Konica business class network printer

Logicube Falcon Neo

Logicube Writebay Protect

Ditto Field Kit

Dell N2048P 10gb 48 port switch

dell poweredge r720

8 6TB HDD 7.2k Storage drives

Fortinet Fortigate Firewall

HTI group Spectrum analyzer

Digital camera

External CD/DVD drive

Spare Components and tools

20 Sata Cables

20 IDE cables

20 Cat E cables

Set of atleast 2 Spare Mouse and Keyboard sets

4 Precision screwdriver sets

Network Cable tester

Network cable punch kit

40 flash drives (Atleast 64GB) (Many will be used for Legacy OS)

20 32GB SD cards

20 HDD (Atleast 500GB in size)

1 500 pack blank CD or DVD R

Firewire and USB adapter kit

AntiStatic bags

Antistatic wrist strap and mat set

Ribbon cables for floppy disks

3 spare SCSI cards

Software

Sophos Antivirus

Encase

FTK

Black Bag

Autopsy

Wireshark

Putty

Various Windows OS including legacy

Linux Kali

Mac OS Versions Currant and Legacy

Paladin

Network Miner

X-ways

Sift

Prodiscover

COFEE

xplico

Encrypted Disk Detector

WinHex

Visual studio

Word Perfect

Quicken

Perl

Python

WPS office

Microsoft office

4 Precision screwdriver sets

Network Cable tester

Network cable punch kit

40 flash drives (Atleast 64GB) (Many will be used for Legacy OS)

20 32GB SD cards

20 HDD (Atleast 500GB in size)

1 500 pack blank CD or DVD R

Firewire and USB adapter kit

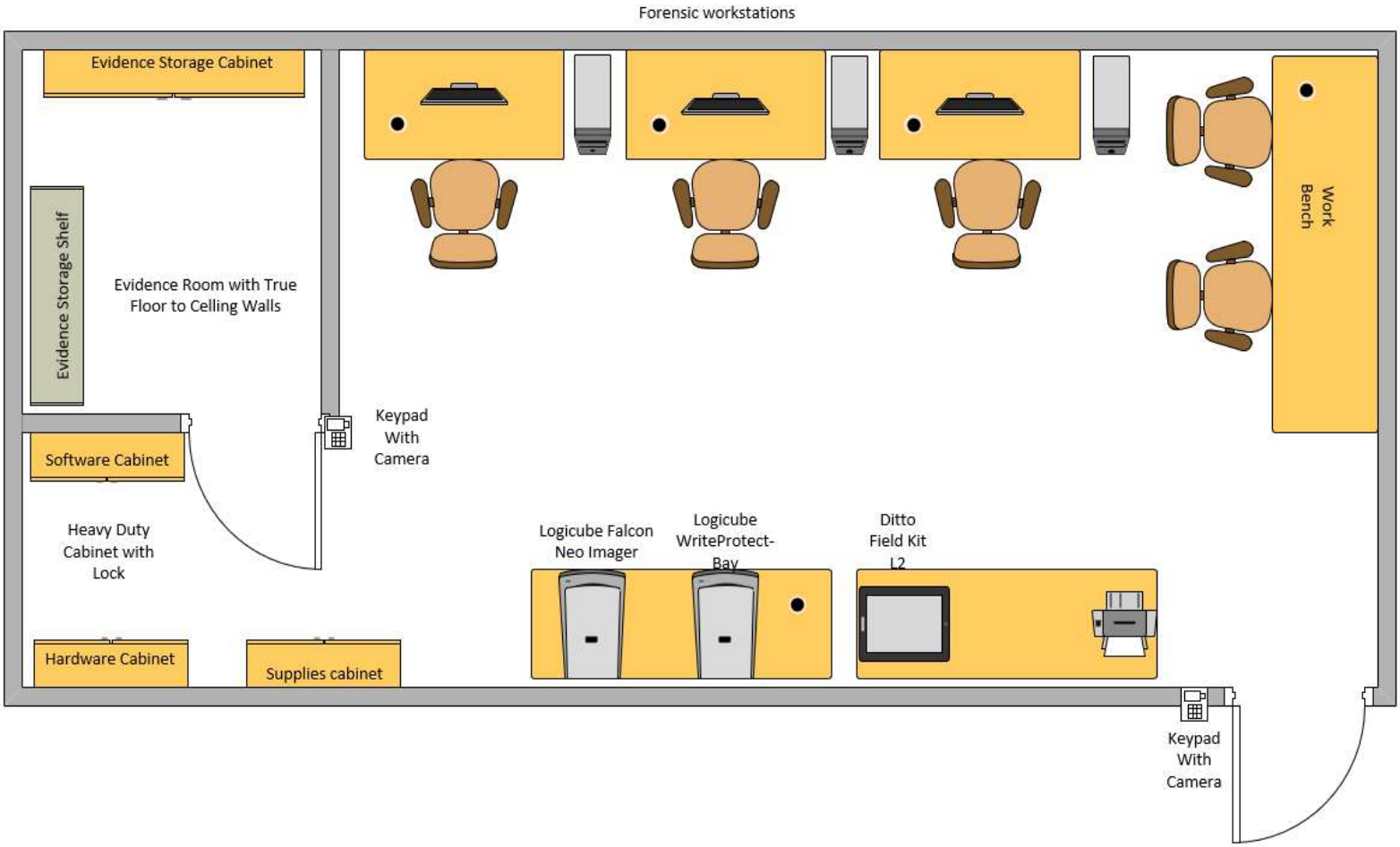
Antistatic bags

Antistatic wrist strap and mat set

Ribbon cables for floppy disks

3 spare SCSI cards

Article IV. Lab Floor Plan



Works Cited and resources

ACCREDITATION MANUAL for INSPECTION, LABORATORIES, and RELATED ACTIVITIES (NON-FORENSIC).

NATIONAL COMMISSION on FORENSIC SCIENCE Views of the Commission Critical Steps to Accreditation Subcommittee Date of Current Version.

Quality Manager, NCSCL. *Sectional Internal Audit Checklist*. North Carolina State Crime Labratory, 21 June 2019.