SWGDE Overview of the Accreditation Process for Digital and Multimedia Forensic Labs

Disclaimer:
As a condition to the use of this document and the information contained therein, the SWGDE requests notification by e-mail before or contemporaneous to the introduction of this document, or any portion thereof, as a marked exhibit offered for or moved into evidence in any judicial, administrative, legislative or adjudicatory hearing or other proceeding (including discovery proceedings) in the United States or any Foreign country. Such notification shall include: 1) The formal name of the proceeding, including docket number or similar identifier; 2) the name and location of the body conducting the hearing or proceeding; 3) subsequent to the use of this document in a formal proceeding please notify SWGDE as to its use and outcome; 4) the name, mailing address (if available) and contact information of the party offering or moving the document into evidence. Notifications should be sent to secretary@swgde.org.

It is the reader's responsibility to ensure they have the most current version of this document. It is recommended that previous versions be archived.

Redistribution Policy:
SWGDE grants permission for redistribution and use of all publicly posted documents created by SWGDE, provided that the following conditions are met:

1. Redistribution of documents or parts of documents must retain the SWGDE cover page containing the disclaimer.
2. Neither the name of SWGDE nor the names of contributors may be used to endorse or promote products derived from its documents.
3. Any reference or quote from a SWGDE document must include the version number (or create date) of the document and mention if the document is in a draft status.

Requests for Modification:
SWGDE encourages stakeholder participation in the preparation of documents. Suggestions for modifications are welcome and must be forwarded to the Secretary in writing at secretary@swgde.org. The following information is required as a part of the response:

a) Submitter's name
b) Affiliation (agency/organization)
c) Address
d) Telephone number and email address
e) Document title and version number
f) Change from (note document section number)
g) Change to (provide suggested text where appropriate; comments not including suggested text will not be considered)
h) Basis for change

SWGDE Overview of the Accreditation Process for Digital and Multimedia Forensic Labs
Version: 1.0 (February 21, 2017)
This document includes a cover page with the SWGDE disclaimer.
Page 1 of 9

Intellectual Property:

Unauthorized use of the SWGDE logo or documents without written permission from SWGDE is a violation of our intellectual property rights.

Individuals may not misstate and/or over represent duties and responsibilities of SWGDE work. This includes claiming oneself as a contributing member without actively participating in SWGDE meetings; claiming oneself as an officer of SWGDE without serving as such; claiming sole authorship of a document; use the SWGDE logo on any material and/or curriculum vitae.

Any mention of specific products within SWGDE documents is for informational purposes only; it does not imply a recommendation or endorsement by SWGDE.

SWGDE Overview of the Accreditation Process for Digital and Multimedia Forensic Labs
Version: 1.0 (February 21, 2017)
This document includes a cover page with the SWGDE disclaimer.
Page 2 of 9

SWGDE Overview of the Accreditation Process for Digital and Multimedia Forensic Labs

Table of Contents

SWGDE Overview of the Accreditation Process for Digital and Multimedia Forensic Labs
Version: 1.0 (February 21, 2017)
This document includes a cover page with the SWGDE disclaimer.
Page 3 of 9

1. Purpose

The purpose of this document is to provide guidance for the ISO/IEC 17025 or 17020 accreditation process. A related SWGDE document, currently in draft, *Framework of a Quality Management System for Digital and Multimedia Evidence Forensic Science Service Providers*, lists key items for a Quality Management System for Digital and Multimedia Evidence Forensic Science Service Providers (DME FSSPs).

2. Scope

This document applies to DME FSSPs who are considering or have chosen to become accredited. While it is recognized that DME organizations vary in size, the core concepts of quality assurance remain the same.

3. What is Accreditation

Accreditation is an independent evaluation by a certified assessment body of a laboratory against recognized standards to carry out specific activities to ensure their competence, impartiality, and compliance. Through the application of national and international standards, stakeholders can have confidence in the results and reports.

Accreditation serves to independently verify that a laboratory is competent to produce reliable results. Accreditation addresses whether a laboratory is using reliable methods, appropriate equipment and software, competent personnel, and drawing reasonable conclusions.

Objectives of accreditation include:

- Improving quality of laboratory services to customers and stakeholders.
- Providing documentation that laboratories meet established standards.

3.1 Definitions

Accreditation – The procedure by which an authoritative body gives formal recognition that a lab is competent to carry out specified tasks.

Accreditation body – An organization conducting and administering an accreditation system.

SWGDE Overview of the Accreditation Process for Digital and Multimedia Forensic Labs
Version: 1.0 (February 21, 2017)
This document includes a cover page with the SWGDE disclaimer.
Page 4 of 9

4.   Accreditation Process

4.1   Phase 1: Self-Assessment

It is important to begin the accreditation process by conducting a high-level overview assessment of your laboratories' needs and benefits of accreditation. During the self-assessment, a laboratory must answer the following questions.

1. Why do we want to be accredited?
    - <u>Action Item</u> – Analyze the benefits and needs: The laboratory should make a list of advantages or reasons for obtaining accreditation. This will assist in the self-assessment decisions below. Part of the list should be focused on the operational aspects of the laboratory for determining the scope of accreditation. This analysis will include such considerations as mandates, stakeholder service requirements, and whether the laboratory can improve its services.

2. What standard do we want to accredit to?
    - <u>Action Item</u> – Select a Standard: Once the decision for pursuing accreditation has been established, the laboratory can determine the appropriate standard, ISO 17025 or 17020. Both standards have been the foundation for digital laboratories developing and implementing a quality management system although 17025 has been the standard chosen by digital laboratories. Another consideration on which standard to select may be that the digital laboratory is part of an organization that has a "traditional" forensic laboratory that has been accredited. In such a case, the digital laboratory may leverage the work done by the affiliate laboratory by adopting many of the policies and procedures for laboratory operations (e.g., reporting and evidence management) and administration (e.g., internal audits and corrective actions).

3. What accrediting body (AB) do we want to conduct our accreditation process?
    - <u>Action Item</u> – Select an Accreditation Body: There are currently two (2) AB, each with their own supplemental requirements:
        a. ANSI-ASQ National Accreditation Board (ANAB). Note: The American Society of Crime Laboratory Directors/Laboratory Accreditation Board (ASCLD/LAB) has merged ASCLD/LAB into ANAB.
        b. American Association for Laboratory Accreditation (A2LA).

4. What customer service needs apply to the laboratory scope of accreditation (e.g. computers, audio, video, mobile, image analysis, etc.)?
    - <u>Action Item</u> – Identify Services to be Accredited: After analyzing reasons for accreditation, customer needs, laboratory operations (current case load / request), resources, etc., the laboratory should decide the scope(s) of accreditation to pursue. An incremental approach may be used with more than one sub-discipline or scope.

SWGDE Overview of the Accreditation Process for Digital and Multimedia Forensic Labs
Version: 1.0 (February 21, 2017)
This document includes a cover page with the SWGDE disclaimer.
Page 5 of 9

5. What are the appropriate industry best practices (e.g., methods, policies, procedures, etc.) that align with our desired scope of accreditation?
   - Action Item – Identify Potential Sources of Best Practices: For example, SWGDE publishes industry best practices for technical methods, laboratory operations, and accreditation. DHS has published test reports on forensic hardware and software. See https://www.dhs.gov/science-and-technology/nist-cftt-reports. Academic researchers have published papers on forensic hardware, software, and methodologies.
6. How much effort is this going to need?
   - Action Item –Conduct a high-level assessment of the current state of the organization's practices to approximate the level of effort to achieve accreditation.
7. Does your management support laboratory accreditation?
   - Action Item – Laboratory management should discuss support for accreditation with the organization's management.
8. Does the laboratory have realistic expectations for accreditation?
   - Action Item – Manage Expectations via Effective Communications: Communicate and set a realistic timeframe of management expectations for accreditation.

4.2   Phase 2: Identify Level of Conformance – Results of Self Evaluation

The next major step is to conduct an analysis of the current level of conformance to the accreditation standards and industry best practices.

The first major activity in this step is to gather lab policies, procedures and other documentation. This will be used to ascertain the current state of lab practices and compare it to the target state. To do this, you will also need to have an understanding of current lab practices. In other words, you are defining your current state and conducting an assessment to identify areas that will need to be improved.

   - Action Item: Create a checklist or other rubric that captures all of the quality management system requirements aligned with appropriate ISO standards and the accrediting body supplemental to achieve accreditation.
   - Action Item: Identify lab documentation that addresses these requirements. Examples of documentation include lab training manuals, operation manuals, quality process manuals, checklists, report templates, and training records.

The second major activity is to analyze the data collected from the self-assessment and compare it to the current practice.

   - Action Item: Evaluate lab practices to determine the level of conformance to accreditation standards and industry best practices. For instance, documented evidence handling and imaging procedures may not account for all types of evidence the lab receives, e.g., damaged media. However, informal practices may exist.

SWGDE Overview of the Accreditation Process for Digital and Multimedia Forensic Labs
Version: 1.0 (February 21, 2017)
This document includes a cover page with the SWGDE disclaimer.
Page 6 of 9

- Action Item: Evaluate lab personnel practices including training programs and competency measurement methods (including mentorship, certification, and internal or external testing).
- Action Item: Create a list of practices to be documented and practices that need to be either improved, developed or implemented. For instance, procedures developed for media acquisition may need to be updated to address new device types, e.g., vehicle infotainment systems or internet of things, embedded devices.

4.3 Phase 3: Bridge the Gap – Action Plan/Schedule

During the initial accreditation process, deficiencies and non-conformances are often identified and bridging the gap is necessary. To do so, the deficiencies and non-conformances need to be prioritized and addressed. Prioritization needs to be done based on the severity of the non-conformance. Prioritization may cause laboratories to consider incremental accreditation such as accrediting computer forensics in year 1 and video in year 2.

- Actions Item: Prioritize the "gaps" based on the requirements for the laboratory to include the following:
  1. Evidence handling
  2. Methods (SOPs, validation, etc.)
  3. Competency
  4. Casework documentation
  5. Equipment/Software control (performance verification)
  6. Laboratory administration and operations
- Action Item: Engage internal and external resources (e.g., accredited government or private labs) for assistance.
- Action Item: Develop milestones to be put into place to remediate the non-conformances. Milestones may include the following:
  1. Writing policies and procedures
  2. Outsource/ Consulting Resources
  3. Develop training for quality system
  4. Potential reorganization of internal structure/workflow
  5. Identify funding needs and resources
- Action Item: Develop an internal and external assessment plan for continual improvement of the lab and the methods.

4.4 Phase 4: Implementation

Having defined the operating policies, procedures and practices, the organization should implement a program of training and integration into operations. Personnel should understand their responsibilities and receive appropriate training to be functionally competent.

SWGDE Overview of the Accreditation Process for Digital and Multimedia Forensic Labs
Version: 1.0 (February 21, 2017)
This document includes a cover page with the SWGDE disclaimer.
Page 7 of 9

▪ Action Item: Develop and implement a training program for the quality management system.

Training needs will vary based on the size of the lab. It is important that all personnel understand and have access to the quality management system documentation. Sample topics that may require staff training include the following:

- Evidence Management
- Casework Documentation
- Reporting and Testimony

4.5   Phase 5: Conformance Documentation

During this phase, the laboratory measures its success at implementing a quality management system and ensures that all relevant documentation exists. This documentation establishes that the laboratory has evidence of conformance to the ISO standard and the organization's own policies and procedures. Documentation requirements fall into three major categories: 1) Policies and Procedures 2) Resources (e.g., people, equipment, facilities) 3) Performance.

▪ Action Item: Document conformance to the accreditation standard.

SWGDE Overview of the Accreditation Process for Digital and Multimedia Forensic Labs
Version: 1.0 (February 21, 2017)
This document includes a cover page with the SWGDE disclaimer.
Page 8 of 9

Scientific Working Group on Digital Evidence

SWGDE Overview of the Accreditation Process for Digital and Multimedia Forensic Labs

History

Revision	Issue Date	Section	History
1.0 DRAFT	2016-09-15	All	Initial draft created and SWGDE voted to release as a Draft for Public Comment.
1.0 DRAFT	2016-10-08	All	Formatted and technical edit performed for release as a Draft for Public Comment.
1.0	2017-02-21	1 and 2	Made changes to the language in *Purpose* and *Scope* for clarity. SWGDE voted to publish as an Approved document (Version 1.0).
1.0	2017-02-21	Formatting	Formatted and published as Approved Version 1.0.

SWGDE Overview of the Accreditation Process for Digital and Multimedia Forensic Labs
Version: 1.0 (February 21, 2017)
This document includes a cover page with the SWGDE disclaimer.
Page 9 of 9