BDCS -03-11
Issue 1: August,2011

Evaluation Criteria and Report

for

Assessment of Biometrics Device Test Laboratory

Information about the laboratory

1. **Name of the Laboratory:**

2. **Address of the Laboratory:**

3. **Contact Person:**

4. **Date of Assessment:**

5. **Assessment Team:**

6. **Scope of Approval:**

Assessment of Biometrics Device Test Laboratory

1.0 Purpose

Purpose of this document is to lay down specific criteria for evaluating competency of Biometrics Device Test Laboratory(BDTL). Some of these requirements are interpretation of equivalent requirement of ISO/IEC 17025. The purpose of this document is not to replace requirements of ISO/IEC.

2.0 Objective and Scope

Objective of this document is to harmonize assessment criteria for Biometric Device Test Laboratory so that consistency can be maintained while evaluating competency of a BDTL. The present scope is testing of Finger print Scanner and Iris Camera for enrolment as well as authentication

3.0 Normative Document

i) NIST HANDBOOK 150-25 CHECKLIST BIOMETRICS TESTING PROGRAM

ii) ISO/IEC 17025: 2005

4.0 Instructions to the Assessor

This document addresses specific approval and reporting requirements for BDTL. Assessor shall support Conformity or non-conformity with comments

5.0 Assessment process

Activities prior to initial on-site assessment

The quality manual and related documentation shall contain or refer to documentation that describes and details the implementation of procedures covering all of the technical requirements .

6.0 Proficiency testing

6.1 Demonstration of SUT (System Under TEST) conformance testing proficiency

The laboratory shall perform a conformance test of a specially designed artifact, referred to as SUT, with one or more features that is/are not in conformance with the standard. The laboratory shall discover the nonconformities, document them, and indicate which standard's requirements have failed due to the presence of the nonconformities.

Deficiencies identified by proficiency testing during an on-site assessment, a scheduled proficiency testing, or submission of incomplete or inaccurate test reports shall be resolved by the laboratory in order to attain or maintain approval.

6.2 *Conflict of interest*

In order to ensure independence of the testing, neither the candidate laboratory nor other divisions within its parent corporation shall provide consulting services for the products that the laboratory tests (e.g., develop testing evidence, design advice, etc.).

6.2.1 For any other services of the laboratory's parent corporation not listed , the laboratory shall have an explicit policy and a set of procedures for maintaining a strict separation, both physical and electronic, between the laboratory testers and company's consultant teams, product developers, system integrators, and others who may have an interest in and/or may unduly influence the testing outcome. The laboratory shall have no financial interest for the work performed under the present scope of approval other than its conformance testing fees.

Auditors comment

7.0 Management requirements for approval Organization

The laboratory shall establish and maintain policies and procedures for maintaining laboratory impartiality and integrity in the conduct of biometrics products testing. To avoid any conflict of interest, the laboratory policies and procedures shall ensure that neither the applicant laboratory nor other divisions within its parent organization can perform conformance testing if it is currently providing or has previously provided consulting services to the vendor for the SUT (e.g., develop testing evidence, design advice).

NOTE :A biometrics laboratory may perform consulting services to provide clarification of the standards, the Derived Test Requirements, and other associated documents at any time during the life cycle of the SUT.

7.1 For any other services of the laboratory's parent organization not listed the laboratory shall have an explicit policy and a set of procedures for maintaining a strict separation, both physical and electronic, between the laboratory testers and company's consultant teams, product developers, system integrators, and others who may have an interest in and/or may unduly influence the testing outcome.

A biometrics laboratory shall have no financial interest in the work performed under the present scope of approval other than its conformance testing fees.

7.2 The laboratory shall not perform conformance testing on a module for which the laboratory has:

- designed any part of the SUT,
- developed original documentation for any part of the SUT,
- built, coded or implemented any part of the SUT, or
- had any ownership or vested interest in the SUT.

NOTE Provided that a biometrics laboratory has met the other requirements, the laboratory may perform conformance testing on SUT produced by a company when:

- the laboratory has no ownership in the company,
- the laboratory has a completely separate management from the company, and
- business between the biometrics laboratory and the company is performed under
- contractual agreements, as done with other clients.

7.3 A biometrics product testing laboratory may take existing vendor documentation for an existing SUT (post-design and post-development) and consolidate or reformat the existing information (from multiple sources) into a set format. If this occurs, the vendor shall be notified of this action when the conformance test report is submitted.

7.4 For additional guidance on laboratory organization, and interpretations and clarifications concerning conflict of interest and strategies for avoiding it, the laboratory shall also consult the guidance provided by TAC, when applicable. If any discrepancy in the provided information regarding the approval process and/or conflict of interest arises, Management committee instructions and policies supersedes the documentation provided by TAC.

7.5 Management system

The laboratory shall complete the cross-reference section of the applicable checklists allowing the laboratory and assessor(s) to verify that all requirements of this checklist and ISO 17025 are addressed and their locations clearly identified in the management system documentation.

7.6 The management system shall provide policy and procedures to ensure routine checks of the competence of the staff involved in the conduct and evaluation of the biometrics products testing.

7.7 Document control

Data collected for biometrics testing is also identified as “Personally Identifiable Information” (PII) and shall be properly collected, stored, transported, transmitted and disposed of such that the information is not disclosed to unauthorized parties. PII information can include both paper and electronic formats in any information system.

7.8 The laboratory shall implement policies and procedures for handling and properly safeguarding the PII that address safeguarding data at rest, properly protecting any PII data in transfer, and disclosure of any PII data. The policies and procedures should be in compliance with all laws e.g., IT Act including amendments that address "acceptable uses" of PII and shall be included in the quality manual and/or related documents.

NOTE As a safe harbor, laboratories could limit the risk of PII disclosure by:

- unless encrypted, prohibiting mobile devices use for storing, transferring or transmitting PII data; implementing multi-factor authentication for access to the PII data when remote access to the database cannot be avoided;
- encrypting the databases that contain PII, whenever database size permits it; when database size does not allow full data encryption, splitting PII data into indirect data elements that cannot identify individuals when stored in separate databases.

When applicable, the quality manual and related documentation shall include procedures and policies for handling software and maintaining the software's integrity according to the copyright and secrecy status.

7.9 Review of requests, tenders and contracts

The contract review shall be conducted to ensure that a laboratory is capable of providing the service, and that the requirements, rights, and responsibilities of the parties are understood.

If the laboratory conducts testing at client sites or any selected site other than the laboratory's site accredited for conformance testing, the site shall meet all requirements pertinent to the conformance testing of the SUT as the approved testing laboratory.

NOTE The laboratory may use checklists and/or contract agreements to satisfy this requirement

7.10 The laboratory shall establish and maintain documented procedures for the review of contracts between the laboratory and clients. Policies for document storage and maintenance of contract under confidentiality or non-disclosure agreements, marked as secret, or copyright protected, shall be defined according to the document's status. These documents shall be protected commensurate with their classification and/or sensitivity, and access to them shall be given only to authorized personnel.

The testing laboratory and client shall agree in writing what constitutes the SUT and what constitutes the environment within the SUT. For this program, the environment includes, but is not limited to:

- the specific test platform,
- the test configuration, and
- the external environment.

7.11 Subcontracting of tests and calibrations

If subcontracting is used as a mechanism by which the laboratory fulfills and/or enhances the conformance testing process, the laboratory shall employ either services provided by NABL-accredited laboratories or by laboratories that satisfy all testing requirements and all documents provided by TAC, when applicable. In the latter instance, the subcontracting laboratory:

a) shall justify the selection explaining why this particular subcontractor was selected and how the subcontractor satisfies the testing requirements, and

b) shall assume full responsibility for the outcome of the conformance testing performed by the subcontractor.

7.12 Control of records

General

The laboratory shall maintain a functional record-keeping system for each client. Records shall be readily accessible and complete. Digital media shall be logged and properly marked, and they shall be properly and securely backed-up. Entries in paper-based laboratory notebooks shall be dated and signed or initialed.

Digital records shall contain entries of pertinent staff/date information for data as required in the quality manual and, as an established safeguard, shall have means to preserve integrity of records, and shall have means for maintenance without later unauthorized modifications.

7.13 Software and data protected by non-disclosure agreements or classified as confidential shall be stored according to the vendor and/or government requirements and commensurate with the data sensitivity, and access shall be granted only to the authorized personnel. An access log file shall be maintained.

The testing laboratory shall take steps to ensure that no third party can gain access to on-line records or to hard copies of the records, either during, or after testing.

If a client's system on which testing is conducted is potentially open to access by third parties, the testing laboratory shall ensure that the client controls the testing environment so that the third parties do not gain access to that system during testing.

Records of all management system activities, including training, internal audits, and management reviews, shall be securely saved for future reviews. The integrity of electronic documents shall be assured by means commensurate with the data sensitivity. Documents in hard copy form shall be marked and stored in a secure location. If necessary to preserve a document's integrity and prevent unauthorized changes, a file logging any access, change, or addition to the document shall be maintained.

Laboratories shall maintain records of the configuration of test equipment and all analyses to ensure the suitability of test equipment to perform the desired testing.

7.14 Technical records

The final test results and/or the test reports generated for the SUT, using biometrics testing tools or biometrics data, shall be kept by the laboratory following the completion of testing for the life of the SUT, or as specified by the client in writing. Records may include hard or digital copies of the official test results and the test results error file(s).

7.15 Internal audits

The internal audit shall cover compliance with NABL laboratory management system, contractual, testing, and test method requirements.

7.16 An applicant laboratory shall conduct at least one complete internal audit, including the test methods that are requested to be on the laboratory's scope of accreditation, prior to

the first on-site assessment. The internal audit report and pertinent records will be reviewed by the STQC assessor before or during the pre-approval on-site assessment.

7.17 For approved laboratories, reports and pertinent records for internal audits conducted since the previous on-site assessment shall be made available for review during the on-site assessment.

Auditors comment

8.0 Management reviews

Periodic reviews of the management system shall reflect adherence to NABL requirements and the laboratory's quality objectives.

Management reviews shall review all nonconformities and may reflect positive aspects of the management system.

An applicant laboratory shall perform at least one complete management review prior to the first on-site assessment. The management review report(s) and pertinent records will be reviewed by the STQC assessor before or during the pre-approval on-site assessment.

For accredited laboratories, reports and pertinent records for management reviews conducted since the previous on-site assessment shall be made available for review during the on-site assessment.

8.1 Technical requirements for approval

Personnel

The laboratory shall maintain competent administrative and technical staff that are:

a) knowledgeable of all biometrics standards and publications listed as references in this handbook pertaining to the specific tests found on the laboratory's scope(s) of accreditation;

b) familiar with the biometrics terminology, biometrics modalities, biometrics systems and sub-systems;

c) familiar with the "acceptable use" (collection, storage, handling, etc.) of the PII as described in the laws;

d) familiar with the biometrics products testing protocols, procedures and tools, when applicable;

e) familiar with human-crew interaction and human-crew rights and responsibilities, when applicable.

8.2 The laboratory shall maintain a list of personnel designated to fulfill NABL requirements including:

a) laboratory's director;

b) Authorized Representative;

c) Approved Signatories;

d) team leaders;

e) key technical persons in the laboratory.

NOTE Significant changes in a laboratory's key technical personnel or facilities may result in a STQC monitoring visit, and/or suspension of accreditation if the new personnel or facilities prove to be inadequate.

The laboratory shall identify a staff member as quality manager with overall responsibility for quality assurance and for maintenance of the quality manual. An individual may be assigned or appointed to serve in more than one position; however, to the extent possible, the laboratory director and the quality manager positions should be independently staffed.

The quality manager shall receive management system training, preferably in ISO/IEC 17025. If training is not available in ISO/IEC 17025, training should be acquired in the ISO 9000 series, especially ISO 9001, or equivalent with particular emphasis on internal auditor training.

8.3 Laboratories shall document the required qualifications for each staff position. The staff information may be kept in the official personnel folders or in separate folders that contain only the information that the STQC assessors need to review.

8.4 The laboratory key technical personnel who conduct biometrics products testing activities shall have at least a Bachelor of Science in Computer Science, Computer Engineering, Electrical Engineering, Human Factors or similar technical discipline or equivalent experience.

8.5 Laboratory staff collectively shall have knowledge of or experience in the following areas:

a) biometrics modalities available;
b) design/analysis of biometrics systems and sub-systems;
c) database systems;
d) biometrics products testing protocols and procedures;
e) biometrics data structures;
f) biometrics standards and special publications referenced in this handbook;
g) familiarity with operating systems under which the biometrics systems are operating;
h) any specific technology upon which testing is conducted.

8.6 The laboratory shall have documented a detailed description of its training program for new and current staff members. Each new staff member shall be trained for assigned duties. The training program shall be updated and current staff members shall be retrained when relevant standards or scope of accreditation changes, or when the individuals are assigned new responsibilities. Each staff member may receive training for assigned duties either through on-the-job training, formal classroom study, attendance at conferences, or another appropriate mechanism. Training materials that are maintained within the laboratory shall be kept up-to-date.

8.7 The laboratory shall have a competency review program and procedures for the evaluation and maintenance of the competency of each staff member for each test method the staff member is authorized to conduct. An evaluation and an observation of performance shall be conducted annually for each staff member by the immediate supervisor or a designee appointed by the laboratory director. A record of the annual evaluation of each staff member shall be dated and signed by the supervisor and the employee. A description of competency review programs shall be maintained in the management system.

8.8 If the mechanism by which the laboratory employs staff members is through contracting, any key personnel who are contractors shall be identified and listed in the laboratory's application for accreditation. When a change in the key personnel employed through contracting occurs or when the direct supervision of this category of personnel is not possible, a report shall be submitted to STQC.

NOTE Any of the above-listed changes in the personnel employed through contracting can affect a laboratory's approval status.

8.9 STQC does not make a distinction between laboratory employees and individuals hired under a contracting agreement. STQC requires that the laboratory maintain responsibility for and control of any work performed within its scope of approval. To that end, the laboratory shall ensure all individuals performing evaluation activities satisfy all STQC requirements, irrespective of the means by which individuals are compensated (e.g., the laboratory shall ensure all test personnel receive proper training and are subject to annual performance reviews, etc.).

8.10 The laboratory personnel who handle PII documents shall obey all laboratory policies and procedures that implement the federal and state privacy laws that stress the "acceptable uses" of PII.

8.11 The laboratory shall have adequate facilities to meet the requirements for STQC approval. This includes facilities for security conformance testing, record-keeping, document storage, and hardware and software storage. The laboratory shall have access to staff training facilities.

8.12 A protection system shall be in place to safeguard customer proprietary hardware, software, test data, electronic and paper records, and other materials. This system shall protect the proprietary materials and information from personnel outside the laboratory, visitors to the laboratory, laboratory personnel without a need to know, and other unauthorized persons. Laboratories shall have systems (e.g., firewall, intrusion detection) in place to protect internal systems from unauthorized, malicious external entities. If testing activities are conducted at more than one location, all locations shall meet Security

requirements and mechanisms shall be in place to ensure secure communication between all locations.

8.13 If the laboratory is conducting multiple simultaneous test campaigns, it shall maintain a system of separation between the products of different customers and between different products. This includes the product being tested, the test platform, peripherals, documentation, electronic media, manuals, and records.

8.14 The laboratory shall meet the equipment and environment requirements specific to biometrics testing specified in the test methods.

8.15 If testing activities will be conducted outside of the laboratory, the management system shall include appropriate procedures for testing activities at customer sites or other off-site locations. For example, customer site procedures may explain how to secure the site, where to store records and documentation, and how to control access to the test facility.

8.16 If the laboratory is conducting its testing at the customer site or other location outside the laboratory facility, the environment shall conform, as appropriate, to the requirements for the laboratory environment. If a customer's system on which a testing is conducted is potentially open to access by unauthorized entities during testing, the test laboratory shall control the environment. This is to ensure that the systems are in a defined state compliant with the requirements for the tests before starting to perform test work and that the systems ensure that unauthorized entities do not gain access to the system during testing.

Auditors comment

9.0 Test and calibration methods and method validation

Tests may be conducted at the client or laboratory site or at another mutually agreed upon site. When testing is performed at a client site, all STQC requirements pertaining to equipment and environment as they apply to the tests shall apply. Moreover, only the personnel of the STQC approved laboratory shall perform all actions necessary to administer the tests and record the results, including the loading, compiling, configuring, and execution of any of the mandated testing tools.

9.1 Laboratories shall use the test methods and tests derived from their scopes of approval. 10.2 Equipment .

9.2 For its scope of approval, the laboratory shall have appropriate hardware, software, and computer facilities to conduct biometrics testing. This includes but is not limited to:

a) required software test suites;

b) testing equipment for physical tests;

c) all special equipment necessary to perform all tests derived from the most current version of the standard.

d) Test targets, Test harness and supporting documentation

9.3 The equipment used for conducting biometrics testing shall be maintained in accordance with the manufacturer's recommendations or in accordance with internally documented laboratory procedures, as applicable. Test equipment refers to software and hardware products or other assessment mechanisms used by the laboratory to support the biometrics testing of the SUT.

9.4 When applicable, the laboratory shall own, load and run testing tools provided or validated by an institution indicated by the TAC, and produce test results using such tools, wherever appropriate. When the testing tool is recommended or provided by TAC, the tool may not be altered or changed and shall not be distributed outside the laboratory.

9.5 When applicable, a testing laboratory shall have procedures defining the test to be performed whenever major or minor changes are made to any testing tool. This is necessary to ensure that harmonization is maintained as appropriate with other testing laboratories and that correctness is maintained with respect to the relevant standard(s) or specification(s).

9.6 When a given test tool or equipment configuration must be used but there are no suitable validation services available outside the testing laboratory to which validation is applicable, and no suitable reference implementation that could be used by the testing laboratory to validate the test tool or equipment configuration, then the testing laboratory shall define and document the procedures and methods that it uses to check on the correct operation of the test tool or equipment configuration.

Auditors comment

10.0 Measurement traceability

General

For Biometrics Testing, "traceability" is interpreted to mean that the assessment test tools and test harnesses shall be traceable back to the underlying requirements of the normative standards. This means that each abstract test case and its evaluation methodology are traceable to specific biometrics requirements listed in the governing

documentary standard, and that they are achieved via the assertions and associated Derived Test Requirements documented in the testing tool in use.

Calibration

Test tools

For biometric and security testing purposes, calibration means verification of correctness and suitability. Any test tool used to conduct biometrics testing and which is not part of the SUT shall be evaluated in isolation to make sure it correctly represents and assesses the test assertions it claims. When possible, test tools should also be examined to ensure that they do not interfere with the conduct of the test and do not modify or impact the SUT. Software testing tools, by necessity, alter the runtime environment in which the SUT performs. Therefore, such tools should be examined to ensure minimum impact to the SUT.

Laboratories shall maintain records of the configuration of test equipment and all analyses to ensure the suitability of test equipment to perform the desired testing.

10.1 Test equipment

The equipment used for conducting the conformance tests shall be maintained and recalibrated in accordance with the test tool author's recommendation, if applicable; as specified in the test method; or annually, whichever results in shorter time periods between calibrations.

The reference standards used and the environmental conditions at the time of calibration shall be documented for all calibrations. Calibration records and evidence of the traceability of the reference standards used shall be made available for inspection during the on-site visit.

10.2 Testing

When applicable, confirmation of the most current version of testing tools shall be assured before conducting a test. This may be accomplished through configuration management for all hardware and software, or through software version control. Records shall be kept of the date and extent of all hardware and software upgrades and updates.

Laboratories shall use the test methods in specific test methodology standards or DTRs. When exceptions are deemed necessary for technical reasons, the client shall be informed and details shall be described in the test report. Substantive documentation shall be provided on exceptions taken to the test method and DTRs to ensure that the correct and required precision and interpretation of the test assertion is maintained. When necessary, these reports may be used to update abstract test cases, the testing tool when applicable, and its accompanying documentation.

10.3 Sampling

If a laboratory applies for biometrics scopes of approval that involve testing with human subjects, the laboratory shall implement policies and procedures that:

a) protect the physical and psychological well-being of the human subjects during testing,

b) serve as a safeguard to protect against errors in ethical judgment,

10.4 The laboratory shall submit all policies and procedures defining biometrics products testing with human subjects and all test suites used for this category of biometrics products testing to TRC

10.5 The laboratory shall ensure that the disposition of any intellectual property generated via the sampling of biometrics data from human subjects is compatible with each testing methodology standard, or DTR, and that it complies with vendor's requirements when applicable.

10.6 Handling of test and calibration items

Laboratories shall protect all products under testing and test tools from modifications of any kind and unauthorized access and use. Laboratories shall ensure that export-controlled equipment, such as fingerprint scanners, is protected in accordance with Export Administration Regulations (EAR).

10.7 When the SUT consists of software components, the laboratory shall ensure that a configuration management is in place to prevent unauthorized modifications. This configuration management shall uniquely identify each software component of the SUT and control and document modifications to any of the software components.

Auditors comment

11.0 Reporting the results

General

The laboratory shall issue test reports of its work which accurately, clearly, and unambiguously present the test conditions, the test setup when varies from the standard protocol, the test results, and all other information necessary to reproduce the test. Any deviations or omissions from the standard shall be clearly indicated. Test reports to clients shall meet contractual requirements in addition to meeting the requirements of this document reports

11.1 Test reports

If a STQC/supplied test report tool or other reporting methodologies are provided, the laboratory shall follow those requirements and use those supplied test tools.

Whenever test cases are such that an analysis of the observations by the testing staff is required in order to interpret the results before stating them in a test report, the testing laboratory shall have objective procedures to be followed by the test operators performing the analysis, sufficient to ensure that the repeatability, reproducibility, and objectivity of the test results can be maintained.

Test reports bearing the STQC symbol may be written for more than one purpose:

a) Reports that are produced under contract and intended for use by the client

Reports intended for use only by the client shall meet client/laboratory contract obligations and be complete, but need not necessarily meet all conformity assessment requirements.

b) Reports to be submitted to the vendors for biometrics product conformity assessment

Electronic transmission of conformity assessment test results

A laboratory may submit either a printed or an electronic report as instructed by the vendor. The electronic version shall have the same content as the printed reports and shall be generated using a software application that is acceptable to TAC if the vendor intends to submit the test results for assessment. A controlled copy of the report shall be placed in the laboratory's records. A mechanism that ensures the control copy's integrity and confidentiality commensurable with the data sensitivity and/or programmatic requirements shall exist.

The laboratory shall provide an integrity and confidentiality mechanism commensurable with the data sensitivity and/or programmatic requirements and/or government requirements when electronic delivery of the test reports to the vendor is employed. Confidentiality mechanisms shall be employed to ensure that the test report cannot be disclosed to anyone other than the intended recipient(s), while an integrity mechanism shall exist to ensure that the test report is not maliciously modified.

11.2 Amendments to test reports and calibration certificates

For test reports created for assessment purposes by TAC or any institution designated by TAC, the laboratory shall issue corrections or additions to a test report only by a supplementary document that is suitably marked and that meets TAC's requirements.

11.3 For test reports created for purposes other than official SUT assessment, the laboratory shall issue corrections or additions to a test report only by a supplementary document suitably marked; e.g., "Supplement to test report serial number [...]". If the change involves a test assertion, this document shall specify which test assertion is in question, the content of the result, the explanation of the result, and the reason for acceptance of the result.

Auditors comment

12.0 Additional initial approval requirements

12.1 Additional initial approval requirements covers

Laboratory as a prerequisite shall owe or rent a physical facility with adequate floor space for the size of the required human crew and with adequate physical security commensurable with the collected and/or tested data sensitivity and with the hosted equipment.

12.2 Additional initial approval requirements

A laboratory shall have the capability to execute the statistical analysis methodologies identified by conformity assessment procurement, to determine the confidence intervals to be used in establishing the Pass/Fail recommendation for each specified test metric.

12.3 A laboratory applying for approval shall have the staff experienced or trained in, and possess the tools needed to perform, custom integration of the biometric devices to facilitate automated capture of biometric matching similarity scores. This data (while not absolutely required) should be collected whenever possible to achieve the maximum benefit of the testing results.

Auditors comment

13.0 Additional proficiency testing (PT) requirements

13.1 Additional PT requirements

A laboratory shall demonstrate their capability and proficiency in performing the specific statistical analysis to be applied to the test results to determine confidence intervals for the measured data, and subsequently the Pass/Fail decision relative to the Performance Specifications. This proficiency is tested by executing the statistical analysis methodology, programmed into the laboratory's data analysis processing system.

Auditors comment

14.0 Additional personnel requirements

General

The laboratory's key technical personnel shall be trained or have three years of direct work experience, prior to approval, in the area of biometrics products testing best practice, biometric technologies and events relevant to practicing privacy protection, and possess basic knowledge of:

- biometric matching and template generation algorithms and uses;
- biometric testing harnesses and implementations;
- physical security;
- protection of personally identifiable information;
- identification and authentication technologies and techniques;
- conformance requirements.

The laboratory's key technical personnel shall have experience or be trained prior to approval

Auditors comment

Recommendations of the Auditors