

ASB Best Practice Recommendation 114, First Edition
2020

**Best Practice Recommendations for Internal Validation
of Software used in Forensic DNA Laboratories**



Best Practice Recommendations for Internal Validation of Software used in Forensic DNA Laboratories

ASB Approved Xxxxx 2020

ANSI Approved Xxxxxx 2020



Academy Standards Board
410 North 21st Street
Colorado Springs, CO 80904

This document may be downloaded for free at: www.asbstandardsboard.org

This document is provided by the AAFS Standards Board for free. You are permitted to print and download the document and extracts from the document for your own use, provided that:

- *you do not modify this document or its related graphics in any way;*
- *you do not use any illustrations or any graphics separately from any accompanying text; and,*
- *you include an acknowledgement alongside the copied material noting the AAFS Standards Board as the copyright holder and publisher.*

You expressly agree not to reproduce, duplicate, copy, sell, resell, or exploit for any commercial purposes, this document or any portion of it. You may create a hyperlink to www.asbstandardsboard.org to allow persons to download their individual, free copy of this document. Your hyperlink must not portray AAFS, the AAFS Standards Board, this document, our agents, associates and affiliates in an offensive manner, or be misleading or false. You may not use our trademarks as part of your link without our written agreement for you to do so.

The AAFS Standards Board retains the sole right to submit this document to any other forum for any purpose.

Certain commercial entities, equipment or materials may be identified in this document to describe a procedure or concept adequately. Such identification is not intended to imply recommendations or endorsement by the AAFS or the AAFS Standards Board, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

*This document is copyrighted © by the AAFS Standards Board, LLC. 2019 All rights are reserved.
410 North 21st Street, Colorado Springs, CO 80904, www.asbstandardsboard.org.*

Foreword

This document includes guidelines for the internal validation of software used in a forensic DNA laboratory that impacts the integrity of the evidence, the analytical process, interpretations and/or statistical conclusions. This document is not intended to be exhaustive and does not include specific recommendations regarding all aspects of good software engineering, development and testing. Additional guidelines and standards may be applicable to specialized software packages.

This document was revised, prepared, and finalized as a Best Practice Recommendation by the DNA Consensus Body of the AAFS Standards Board. The draft of this standard was developed by the Biology/DNA Biological Data Interpretation and Reporting Subcommittee of the Organization of Scientific Area Committees (OSAC) for Forensic Science.

The AAFS Standards Board (ASB) is an ANSI-accredited Standards Developing Organization with the purpose of providing accessible, high quality science-based consensus forensic standards. The ASB is a wholly owned subsidiary of the American Academy of Forensic Sciences (AAFS), established in 2015 and accredited by the American National Standards Institute (ANSI) in 2016. The ASB consists of Consensus Bodies (CB), which are open to all materially interested and affected individuals, companies, and organizations; a Board of Directors; and Staff.

The following applies to all ASB documents:

the term **'shall'** indicates that a provision is mandatory, and can be audited for compliance

the term **'should'** indicates that a provision is not mandatory, but recommended as good practice.

All hyperlinks and web addresses shown in this document are current as of the publication date of this document.

Keywords: *Software validation, forensic DNA.*

Table of Contents

1	Scope.....
2	Normative References
3	Terms and Definitions
4	Recommendations.....
5	Conformance.....
	Annex A (informative) Bibliography

DRAFT

Best Practice Recommendations for Internal Validation of Software used in Forensic DNA Laboratories

1 Scope

This best practice recommendation assists a laboratory in designing internal validation studies to evaluate the various software programs used in the forensic DNA laboratory.

This guidance document applies to, but is not limited to the following.

- a) Software used as a component, part, or accessory of instrumentation.
- b) Software that impacts the chain of custody documentation.
- c) Software that impacts the decision process and/or influences conclusions or reporting.
- d) Software created by the laboratory to assist with calculations and/or data transfers.

2 Normative References

The document contains no normative references. See Annex A, Bibliography for other references.

3 Terms and Definitions

For purposes of this document, the following definitions apply.

3.1

boundary testing

Checking to confirm expected outputs are obtained when inputs are at the limits of the software (e.g. testing allele frequencies below the $5/2N$ minimum threshold or testing upper and lower limits for amplification setup calculations).

3.2

complex software

Sophisticated computer programming that contains multiple interconnected modules or components. Complex software systems have components whose interactions evolve. The set of possible states the system can be infinite, unbounded, and most importantly, changing.

3.3

critical software

Any software or modification that directly affects the integrity of the evidence, the analytical process, interpretations, statistical conclusions, case file documentation, chain of custody documentation, accuracy of results, report wording, or any other item deemed integral.

3.4

internal validation

The accumulation of test data within the laboratory to demonstrate that established parameters, software settings, formulae, algorithms and mathematical functions perform as expected; and that the information/results/data obtained is correct and consistent with expected values.

3.5

functional testing

Checking to confirm that the software performs tasks as expected.

3.6

fuzz testing

Checking to confirm that invalid, unexpected or nonsensical inputs to a computer program or module yield an acceptable response (e.g., an error message or other indication of a problem).

3.7

negative testing

Checking to confirm that incorrect or inverse inputs yield the expected output (e.g., inputting a letter when a number is required, and observing an error message).

3.8

operating system

System software that manages computer hardware and software resources and provides common services for computer programs.

3.9

positive testing

Checking to confirm that the natural (or usual) inputs yield the expected output.

3.10

regression testing

Checking to confirm that changes or new functionality does not unacceptably alter or terminate a desired functionality that behaved correctly before the change was implemented.

3.11

reliability testing

Checking beyond the functional aspects to measure the reliability of the software in the laboratory environment. This includes testing the impact on software performance when utilized by multi-user or multi-site scenarios and verifying network, server, and other applicable resources can handle the application's needs.

3.12

risk

An uncertain event or condition that, if it occurs, has a negative effect on a software's reliability and performance.

3.13

risk assessment

A systematic process for deciding the risk level associated with a particular software or module.

3.14

software developer

The legal entity or vendor company which created and/or provides a software program.

**3.15
software module**

Part of a software program. Programs are typically composed of one or more independently developed modules. Modules may be acquired as additions to a software program already in use, or they may be fully integrated into the software program (e.g., add-ins/plugin-ins, and macros).

**3.16
software program**

A set of instructions, modules or procedures, that allow for a certain type of computer operation. Interchangeable terms include “software application” and “software product.”

**3.17
software test**

Individual trial designed to evaluate specific software functions.

**3.18
software test types**

Different categories of trials that comprise the software internal validation.

**3.19
software internal validation**

Confirmation, through the provision of objective evidence, derived from a series of documented tests, of the compliance of a software system with intended use and applicable guidelines.

4 Recommendations

The recommendations listed below apply to internal validation only. For probabilistic genotyping software refer to Standard 018, ANSI/ASB Standard 018, *Standard for Validation of Probabilistic Genotyping Systems*, First Edition, 2020¹.

4.1 New software programs, modules or software modifications, such as a major functionality addition, that impact evidence integrity, the analytical process, the interpretations, and/or statistical conclusions, case file documentation, chain of custody documentation, accuracy of results, report wording, or any other item deemed integral should be validated prior to implementation.

There may be examples of commercial software where the DNA laboratory does not have autonomous control over, such as chain of custody software, for which the DNA section may not be able to validate all of the modules. The DNA section should still validate all of the modules over which they have control, and they should document the extent to which they rely on modules that they are unable to validate.

4.2 The internal validation of the software should be carried out for a given software environment which is recommended by the software developer (e.g., operating system, database management system).

As the computing environment of the software evolves (for example, substantive version changes to the operating system, or fundamental changes to the computing hardware architecture), the

¹ http://www.asbstandardsboard.org/wp-content/uploads/2020/07/018_Std_e1.pdf

consequences should be evaluated and a software risk assessment should be performed. An internal validation should be conducted if applicable based on the outcome of the software risk assessment.

4.3 The forensic laboratory should choose one of the two following internal validation approaches.

4.3.1 The forensic laboratory performs the internal validation of the software. This approach may include documented validations performed by the developer but these, in themselves, are not sufficient.

4.3.2 The forensic laboratory uses a third party to perform the internal validation.

4.4 Internal validation should demonstrate that the software is fit for its intended use in the operational environment and should define its limitations.

NOTE Testing of software provides unique challenges and it is unlikely that a test can be designed for every use-case, or scenario for all software programs or modules. Software associated with an instrument may be validated in conjunction with the instrument.

4.5 When internally validating new software, the laboratory should rely on the software developer to explain the functionality.

4.5.1 The laboratory should require the developer to provide documentation, such as a user's manual, to explain the intended uses and limits of the software.

4.5.2 The laboratory may rely on the results of testing conducted by the developer but the laboratory should also extend tests during their internal validation.

4.6 For software upgrades or modifications, the laboratory should require the developer to provide written documentation, such as release notes, to explain the purpose and scope of the modifications.

4.6.1 Every version of the software should be identified by a unique release number.

4.6.2 Information about recommended internal validation tests to assess the changes may also be requested from the developer.

4.7 The forensic laboratory should design, or ensure that the developer has designed validation tests that evaluate the software's performance and the limits within which it performs properly.

4.7.1 If a third party is used, in whole or in part, to validate the software program or module, the forensic laboratory is responsible for determining that the validation design, testing procedures and documentation meet the recommendations as detailed in this document.

4.7.2 If an internal validation incorporates the results of previously performed testing into the assessment, the forensic laboratory is responsible for determining whether the validation design, testing procedures and documentation meet the recommendations as detailed in this document.

4.7.3 If the recommendations have not been met, the forensic laboratory should identify what additional efforts are needed to establish that the software is sufficiently validated for its intended use in the laboratory.

4.8 Internal validation should follow a predefined plan as depicted in Figure 1.

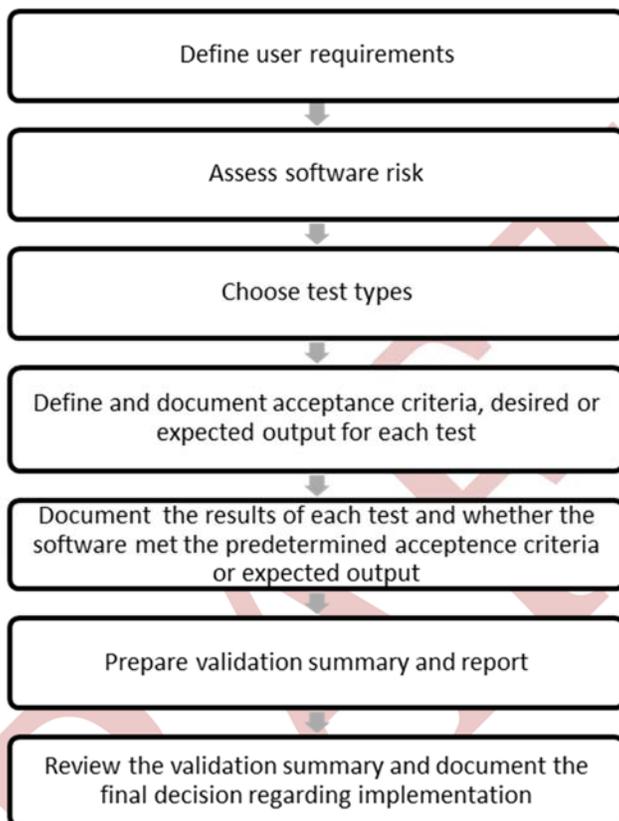


Figure 1—Internal validation Plan

4.8.1 User requirements for the software program and/or module should be defined and documented.

4.8.2 A risk assessment should be performed to make an objective assessment of the level of criticality and complexity of a software program or module. A risk assessment should be conducted whenever a new version of a software program or module is released or when there are software modifications or updates.

4.8.2.1 Critical: Any software or modification that directly affects the integrity of the evidence, the analytical process, interpretations, statistical conclusions, case file documentation, chain of custody documentation, accuracy of results, report wording, or any other item deemed integral.

4.8.2.2 Not Critical: Software that provides information to the analyst that aids the analysis, interpretation, or reporting process, but does not directly affect the analytical process, conclusions, or documentation.

4.8.2.3 Complex: Software that contains many interconnected modules or components. In cases where an already validated software program or module has been updated, the complexity of the change or update should be evaluated based on the complexity of the software modification.

4.8.2.4 Not Complex: A simple software program, module, or upgrade that does not satisfy the definition of complex software. This may include simple spreadsheets or equations easily confirmed by the user.

4.8.3 The recommended software test types should be chosen based upon the determined level of criticality and complexity established during risk assessment. The most complex software programs or modules with the highest level of criticality warrant the highest level of internal validation testing.

4.8.3.1 The following software testing types should be performed during internal validation.

a) Functional software testing including the following sub-types (as appropriate):

- 1) positive testing;
- 2) negative testing;
- 3) boundary testing;
- 4) fuzz testing.

b) Reliability Testing.

c) Regression Testing.

4.8.3.2 The type and number of tests should be based on the risk assessment. The following tests (based on the possible states in Figure 2), at a minimum, are recommended for given criticality/complexity levels.

a) Not Critical/Not Complex (e.g., already validated software with a misspelled word corrected).

- 1) Functional testing: Positive.

b) Critical/Not Complex.

- 1) Functional testing: Positive, Negative, Boundary.
- 2) Regression testing: If applicable (i.e., software updates).
- 3) Reliability testing: If applicable (e.g., multi-user environment).

c) Not Critical/Complex (e.g., updates to module with quality flags used to aid analysis).

- 1) Functional testing: Positive, Negative, Fuzz.
- 2) Regression testing: If applicable (i.e., software updates).

d) Critical/Complex.

1) All Functional, reliability, and regression testing.

	Not Critical	Critical
Not Complex	1. Not Critical Not Complex	2. Critical Not Complex
Complex	3. Not Critical Complex	4. Critical Complex

Figure 2—Software Risk Assessment Decision Matrix

4.8.3.3 Test cases, which are designed to challenge the system and evaluate its performance against predetermined criteria, especially for its most critical parameters, should be created.

4.8.3.3.1 The test cases should cover the full range of operating conditions so that the system can encounter a wide spectrum of conditions and events that will typically be encountered at the user site.

4.8.3.3.2 If a set of test data are used to set parameters and establish initial boundary conditions for acceptable performance, the system should then be tested on a fresh data set. This step is necessary to avoid inadvertently fitting the software performance to the characteristics of a single data set.

4.8.3.3.3 Whenever a new version of the software program or module is released, or when there are software modifications or updates, the changes with reference to the previous version should be identified and their consequences should be evaluated to determine the extent and impact of the change on the entire system. Due to the complexity of software, a seemingly small local change may have a significant system impact.

4.8.3.4 If the laboratory chooses to use or incorporate some aspects of the developer’s validation testing and results as part of their own internal validation, then the laboratory should perform a subset of the evaluations performed by the software developer at the laboratory.

4.8.3.4.1 The forensic lab should additionally conduct some of their own tests to demonstrate that the software was installed properly and functions in the context of their operational environment. This is to make sure that there are no incompatibilities with other applications that might not have been present in the developer’s software environment. This may be facilitated by the software developer or vendor furnishing the user with test data sets to be used for this purpose while providing the user with expected results such that the outputs can be compared. The software may have built-in tests that the laboratory can exercise.

4.8.4 Acceptance criteria should be defined and documented prior to performing the tests.

The acceptance criteria should be chosen based on either documented performance characteristics of the software, or against some known/expected values or outcomes.

4.8.5 The results of each test and whether the software met the predetermined acceptance criteria or expected output should be documented.

4.8.5.1 Failing some of the tests does not necessarily mean invalidation. The laboratory may decide that some failures represent minor inconveniences that do not invalidate the software. Alternatively the laboratory may decide that a single critical or a combination of moderate failures is intolerable and the software cannot be accepted.

4.8.5.1.1 Records of any system failure should be maintained.

4.8.5.1.2 The records should detail whether the failure impacts the software's fitness for use.

4.8.5.1.3 If the failure is one that impacts the software's fitness for use, then the laboratory should document the actions taken to ensure the source of failure was resolved and the test(s) repeated with expected results.

4.8.6 An internal validation summary and report should be prepared.

4.8.6.1 The internal validation summary should objectively confirm whether the software is validated for its intended use.

4.8.6.1.1 The internal validation summary should include, at a minimum, the following information:

- a) organization that conducted testing;
- b) defined user requirements;
- c) risk assessment decision and reasoning;
- d) software name including version number;
- e) test cases:
 - 1) date and time of test(s),
 - 2) operating system,
 - 3) input data;
- f) acceptance criteria;
- g) test result(s);
- h) record of any system failure and actions taken to ensure failure was resolved;
- i) record of formal acceptance or rejection; and

j) date the software was approved for use, if implemented.

4.8.6.1.2 The internal validation summary should be maintained by the laboratory.

4.8.6.2 If the laboratory chose to use a third party testing service, or use the developer's validation testing and results, the laboratory should ensure that an internal validation summary has been prepared and is available on site at the laboratory.

4.9 The laboratory should complete its assessment prior to use on evidence samples, casework reference samples, or database samples.

5 Conformance

Documentation demonstrating conformance with the recommendations described in this document should be signed and dated by the laboratory's DNA technical leader and made readily available in hard copy and/or electronic form for review by an assessor.

DRAFT

Annex A (informative)

Bibliography

This is not meant to be an all-inclusive list as the group recognizes other publications on this subject may exist. At the time this document was drafted, these were the publications available to the working group members for reference. Additionally, any mention of a particular software tool or vendor as part of this bibliography is purely incidental, and any inclusion does not imply endorsement by the authors of this document.

- 1] SES-1:2002, *Recommended Practice for the Designation and Organization of Standards*. Date of Issue: 2002-08-01².
- 2] Federal Bureau of Investigation (FBI). *Quality Assurance Standards for Forensic DNA Testing Laboratories*. 2020³.
- 3] FDA. *General Principles of Software Validation; Final Guidance for Industry and FDA Staff*. January 11, 2012⁴
- 4] DOC 9906 AN/472, *Quality Assurance Manual for Flight Procedure Design; Flight Procedure Design Software Validation*. International Civil Aviation Organization. Vol.3, 2010⁵.
- 5] NPL Report DEM-ES 014, *Software Support for Metrology Best Practice Guide No. 1; Validation of Software in Measurement Systems v. 2.2*. NPL (National Physical Laboratory). January 2007⁶.
- 6] Scientific Working Group on DNA Analysis and Methods (SWGDM). *Validation Guidelines for DNA Analysis Methods*. 2012⁷.
- 7] ISO/IEC 17025, *General Requirements For The Competence Of Testing and Calibration Laboratories*. Third Edition, November 2017⁸.

² Available from: <https://www.ses-standards.org/page/Publications>

³ Available from: <https://www.fbi.gov/file-repository/quality-assurance-standards-for-dna-databasing-laboratories.pdf/view>.

⁴ Available from: <https://www.fda.gov/regulatory-information/search-fda-guidance-documents/general-principles-software-validation>

⁵ Available from: https://www.icao.int/Meetings/PBN-Symposium/Documents/9906_v1_cons_en.pdf

⁶ Available from: <https://www.nist.gov/system/files/documents/2017/05/09/NPL-Best-Practice-Guide-No-1-Validation-of-Software-in-Measurement-Systems-Jan2007.pdf>

⁷ Available from: https://1ecb9588-ea6f-4feb-971a-73265dbf079c.filesusr.com/ugd/4344b0_813b241e8944497e99b9c45b163b76bd.pdf

⁸ Available from: <https://www.iso.org/standard/66912.html>

DRAFT



Academy Standards Board
410 North 21st Street
Colorado Springs, CO 80904

www.asbstandardsboard.org