Forensic Science Regulator
Overseeing Quality

# Forensic Science Regulator

# Guidance

## Method Validation in Digital Forensics

FSR-G-218

Issue 2

# Contents

# 1. Executive Summary

1.1.1 Forensic science is science applied to matters of the law. It is an applied discipline, meaning scientific principles and practices are employed to obtain results that the investigating officers and courts can expect to be shown to be reliable.

1.1.2 Validation involves demonstrating that a method used for any form of analysis is fit for the specific purpose intended, i.e. the results can be relied on. The Criminal Practice Directions V – Evidence. [1] [1] suggest that when determining the reliability of expert opinion, the court takes into account:

> "19A.5 (a) the extent and quality of the data on which the expert's opinion is based, and the validity of the methods by which they were obtained."

1.1.3 Validation is also a key component of the Regulator's Codes of Practice and Conduct as well as a requirement for accreditation to the international standard ISO17020 [2] and ISO17025 [3] and the International Laboratory Accreditation Cooperation (ILAC) publication Modules in a Forensic Science Process - ILAC-G19 [4]. Accreditation includes the assessment by a third party that an organisation has demonstrated compliance with the standards, that the methods it uses are valid and that it is competent to perform them.

1.1.4 Validation is a demonstration of fitness for purpose. The first step is to define what the requirements are in terms of inputs, effects, constraints and desired outputs. Validations that skip this step may miss the key quality issues. Unfocused testing can lead to amassing of data that may or may not increase understanding or give confidence in the method.

1.1.5 Most methods are not entirely new, so for methods adopted/adapted from elsewhere where pre-existing validation data are available the requirement [2] is:

> "When a method has been validated in another organization the forensic unit shall review validation records to ensure that the validation performed was fit for purpose. It is then possible for the forensic unit to only undertake verification for the method to demonstrate that the unit is competent to perform the test/examination."

[1] The Criminal Practice Directions V: Evidence relate to parts 16-23 of the Criminal Procedure Rules.

[2] This is taken from the international guidance document on the application of ISO/IEC 17025 and ISO/IEC 17020 in the forensic science process called ILAC-G19:08/2014.

1.1.6 Truly novel methods, or methods that have no available relevant and reliable validation data, require a more in-depth validation often known as a developmental validation. Such in-depth validations sometimes have collaboration on aspects of the validation study. This becomes a mix of the approach required for novel methods as well evaluating the aspects of validation study performed by the collaborating third party (see Section 6.3).

1.1.7 With the exception of methods that are almost entirely tool operation (for example, a simple USB acquisition tool) [3], most methods will have quality assurance stages, checks and/or even reality checks by an expert. These checks control the risks associated with either a specific part of the method or the entire method.

1.1.8 The objective evidence that the method meets the acceptance criteria for the proposed method is the test data, therefore the selection and design of test to generate this is critical.

1.1.9 Data for all validation studies have to be representative of the real life use the method will be put to. If the method has not been tested before the validation will also need to include data challenges that can stress test [4] the method.

1.1.10 If the method being implemented is an adopted method purporting to have been validated by another organisation, the review includes whether the test material/data selected in the original validation did indeed robustly test the method and tools in a manner that matches the particular end-user requirements. The design of the validation study used to create the validation data must also be critically assessed as part of the review of validation records. The onus is for the organisation using the method (i.e. the forensic unit [5]) to demonstrate validation, although the developer may greatly assist the end user by providing information on the testing that has already been performed.

[3] Tools designed to be used by non-practitioners require validation for that purpose, including to determine the limits of operation and error rates. Not having expert intervention is a risk to be addressed.

[4] See Glossary.

[5] A term used in ILAC-G19 to mean “a legal entity or a defined part of a legal entity that performs any part of the forensic science process”.

1.1.11 The end-user requirement and acceptance criteria will directly influence the data set required to give an adequate assessment of the efficiency, effectiveness and competence to perform the activity. Too simple a data set may give little indication of how the method would perform on real casework. However, a too complex data set, using every eventuality including highly unlikely scenarios, will increase implementation time. Remember, certain caveats may always apply to the activity irrespective of how much testing is conducted or how extensive the data sets.

# 2. Introduction

## 2.1 Purpose

2.1.1 The courts have the expectation that the methods to produce the data that an expert bases their opinion on are valid. [6] Validation is the recognised way of demonstrating this, and method validation is a key requirement for accreditation to the ISO standard BS EN ISO/IEC17025:2017 (referred from here as simply ISO17025). [3] Validation involves demonstrating that the method is fit for the specific purpose intended, and that any limitations are understood and explained. Validation is a central feature of the Forensic Science Regulator's Codes of Practice and Conduct for Forensic Science Providers and Practitioners in the Criminal Justice System (the Codes) and the Regulator has published a general guidance document on validation (FSR-G-201).

2.1.2 This document has been produced to provide guidance and advice on validation stages and how the process can be applied within the digital forensic sciences (digital forensics).

## 2.2 Scope

2.2.1 This document is intended to assist validation in the field of digital forensics in compliance with the Codes and ISO17025.

2.2.2 Digital forensics is to be taken to be the process by which information is:

[6] For example, see the Criminal Practice Directions as amended.

a. Extracted from data storage media (for example, devices, remote storage and systems associated with computing, imaging, video, audio, satellite navigation, communications);

b. Rendered into a useable form;

c. Processed; and

d. Interpreted for the purpose of obtaining intelligence for use in investigations, or evidence for use in criminal proceedings.

2.2.3 All digital forensics methods are expected to be demonstrated to be valid, whether covered in this document or not.

## 2.3 Reservation

2.3.1 Every effort has been made to provide useful and accurate guidance of the requirements contained in the Codes. However, if the guidance supplied here inadvertently implies a lesser requirement than the Codes or ISO17025 require, then the standard rather than this guidance will prevail.

## 2.4 Modification

2.4.1 This is the second issue of this document.

2.4.2 Significant changes to the text have been highlighted in grey.

2.4.3 The modifications made to create issue 2 of this document were, in part, to ensure compliance with The Public Sector Bodies (Websites and Mobile Applications) (No. 2) Accessibility Regulations 2018. [7] Text identified as out-of-date during this accessibility review has either been modified or deleted.

2.4.4 The Regulator uses an identification system for all documents. In the normal sequence of documents this identifier is of the form 'FSR-#-###' where (a) the '#' indicates a letter to describe the type or document and (b) '###' indicates a numerical, or alphanumerical, code to identify the document. For example, the Codes are FSR-C-100. Combined with the issue number this ensures each document is uniquely identified.

[7] To facilitate the operation of the Regulations the following significant changes to sections of the document are noted here. The following sections of the document have been amended: Contents table, 1.1.2, 1.1.3, 1.1.6, 2.1.1, 2.4, 2.4.1, 2.4.2, 2.4.3, 2.4.4.,2.4.5, 2.4.6, 4.2.1, 4.3.1, 4.4.6, 4.4.7, 5.1.1, 6.1.8, 6.1.9, 6.1.10, 7.2.1, 12, 13. The following footnotes have been amended: 1, 7.

2.4.5 In some cases, it may be necessary to publish a modified version of a document (e.g. a version in a different language). In such cases the modified version will have an additional letter at the end of the unique identifier. The identifier thus becoming FSR-#-####.

2.4.6 In all cases the normal document, bearing the identifier FSR-#-###, is to be taken as the definitive version of the document. In the event of any discrepancy between the normal version and a modified version the text of the normal version shall prevail.

# 3. An Introduction to Method Validation in Digital Forensics

## 3.1 Method

3.1.1 A method is a logical sequence of procedures or operations intended to accomplish a defined task. A method includes the interaction of the operator and may include multiple tools or none. For instance, acquiring a forensic image of a hard drive (i.e. a bit-by-bit copy of a hard disk drive) with a tested hard drive imager, write blocker and then using hashing algorithms to verify are not several tools or methods, but part of one method. If the write blocker or hash algorithm were required in other methods they could be validated separately, and brought together in the larger method to verify that it meets the methods requirement.

3.1.2 Any method in science or engineering can be documented. The creation of a draft standard operating procedure is good practice before attempting any validation study, as validation is performed on the final method.

## 3.2 Fit for Purpose

3.2.1 The method must be demonstrated to be fit for purpose, which is defined here as:

Is good enough to do the job it is intended to do, as defined by the specification developed from the end-user requirement.

3.2.2 The end-user requirement is focused on in more detail in Section 4; at the simplest level, it is capturing what the different users of the output of the method require. A simple method may have a short requirements document with only a few factors that that influence the generation of the results. A truly novel method featuring user-developed software may be much larger than that.

## 3.3 Validation

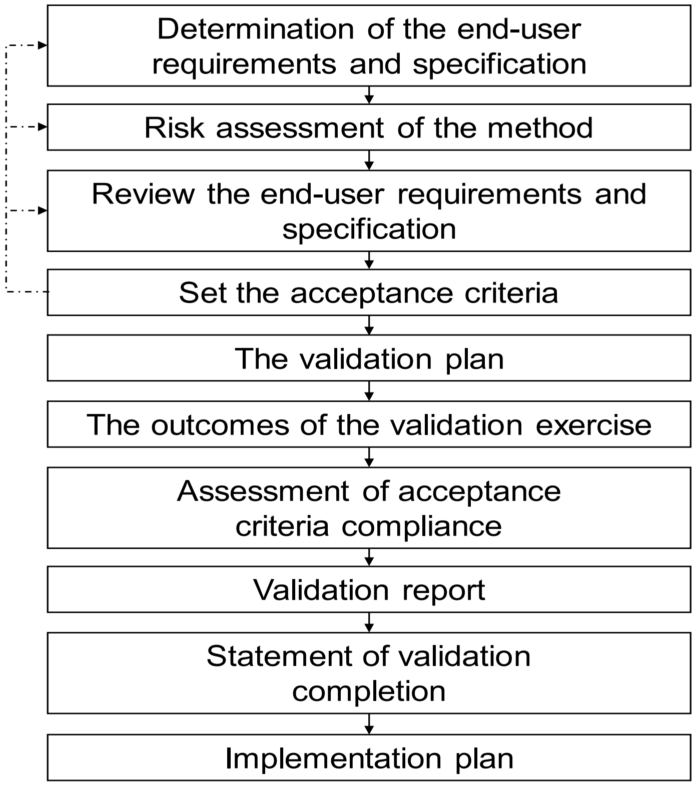
3.3.1 The Regulator defines the validation of scientific methods in the Codes as:

> “The process of providing objective evidence that a method, process or device is fit for the specific purpose intended.”

3.3.2 The validation study may create all the objective evidence required, or it may create some of the objective evidence and collate the remainder from other sources such as scientific literature or other studies. The requirement is for data to be available so that they can be evaluated against the implementing organisation’s end-user requirement.

## 3.4 Summary of the Validation Process

**Figure 1**: Framework published in the Codes


Determination of the end-user requirements and specification
Risk assessment of the method
Review the end-user requirements and specification
Set the acceptance criteria
The validation plan
The outcomes of the validation exercise
Assessment of acceptance criteria compliance
Validation report
Statement of validation completion
Implementation plan

3.4.1 The stages detailed in Figure 1 are expected to be followed whether the method is considered novel or in common use elsewhere. The final validation paperwork should be just as complete whether all the objective evidence of fitness for purpose was created in the study or if much of it was created elsewhere and evaluated against the end-user requirement/ specification as detailed in Section 6.3.

3.4.2 There are no standard methods in digital forensic science. Even though most methods are assumed to be at least in part adopted and/or adapted methods rather than truly novel, for accreditation purposes they are generally referred to as laboratory-developed methods or non-standard methods. Even if a method has been in use for some time, if there are no reliable data on the method then the method may need to be treated more as if it was novel as in Section 6.2.

3.4.3 Following a defined process and compiling the records is required by the Codes, whether conducting a validation study or verifying that the validation studies conducted elsewhere are applicable. It is a linear representation although if lessons are learnt that require changes to the method or validation approach the stages may need repeating or revisiting. In simple methods the paperwork produced could be quite short. However, the validation records should include any external objective evidence used to show that the end-user requirement has been met.

# 4. End-User Requirements

## 4.1 Introduction

4.1.1 The end goal of validation is for the user of the method (the forensic unit), and the user of any information derived from it (the end user), to be confident about whether the method is fit for purpose as well as understanding any limitations. The ability to assess if a method is fit for purpose depends on first defining what the forensic unit needs the method to reliably do, as well as identifying who are the end users of the method and subsequent results.

4.1.2 The requirements, in their simplest form, capture what aspects of the method the expert will rely on for their critical findings, i.e. what the expert needs to provide in a statement or report.

4.1.3 If the method is novel and developed in-house, the user requirement may come from the method development stage. This may be a large document and feature both functional and non-functional requirements. From this the testable functional requirements and acceptance criteria can be identified.

4.1.4 If the method is being adopted or adapted from elsewhere, the end-user requirements will need creating from scratch. Rather than including all the functional and non-functional aspects, the requirements ought to focus on features that affect the ability to give reliable results.

4.1.5 Assurance of the quality of the development of any software tools in a method as well as how the method performs may be a requirement, but it would be onerous to include every function that any software tools used in the method are capable of, and quite irrelevant if the features will not be used.

## 4.2 Identifying the End User(s)

4.2.1 The primary end users of an organisation’s services are often determined by the environment within which it operates. Typically, in digital forensics, forensic units operate within the following environments.

a. A department or unit within a law-enforcement organisation providing forensic services to internal customers within the organisation.

b. A public sector body providing forensic science services to law-enforcement organisations.

c. Service providers, independent consultants or sub-contractors providing services to the prosecution, defence or both.

4.2.2 However, the body instructing the work will rarely be the true end user. If the police request work to be performed in-house, or by an external organisation, the results will have to satisfy their needs as an interim end user. Also, the organisation performing the method will have specific user requirements. Reports and evidence produced will be also be relied on by other bodies within the Criminal Justice System (CJS) and must also meet their requirements. Examples include the prosecuting authorities (for example, Crown Prosecution Service), opposing counsel and the judiciary.

## 4.3 The Court as an End User

4.3.1 The Lord Chief Justice of England and Wales has amended the Criminal Practice Directions [1] to include the following factors in Direction V 19A.5, which the court may wish to take into account in determining the reliability of evidence, many of which are directly relevant to validation.

1. “The extent and quality of the data on which the expert’s opinion is based, and the validity of the methods by which they were obtained.

2. If the expert’s opinion relies on an inference from any findings, whether the opinion properly explains how safe or unsafe the inference is (whether by reference to statistical significance or in other appropriate terms).

3. If the expert’s opinion relies on the results of the use of any method (for instance, a test, measurement or survey), whether the opinion takes

proper account of matters, such as the degree of precision or margin of uncertainty, accuracy or reliability of those results.

4. The extent to which any material upon which the expert's opinion is based has been reviewed by others with relevant expertise (for instance, in peer-reviewed publications), and the views of those others on that material.

5. The extent to which the expert's opinion is based on material falling outside the expert's own field of expertise.

6. The completeness of the information that was available to the expert, and whether the expert took account of all relevant information in arriving at the opinion (including information as to the context of any facts to which the opinion relates).

7. If there is a range of expert opinion on the matter in question, where in the range the expert's own opinion lies and whether the expert's preference has been properly explained.

8. Whether the expert's methods followed established practice in the field and, if they did not, whether the reason for the divergence has been properly explained."

4.3.2 If admissibility is challenged and these factors have not been taken into account, the evidence may be excluded from the proceedings and/or attract adverse comments from the presiding judge. Common law is constantly changing, unlike laws that are codified as Acts of Parliament. Also, legal precedents referring to one evidence type often apply more widely. The Regulator publishes information [5] on legal obligations to assist those acting as expert witnesses in keeping up to date with key case law, although it is only a snapshot.

## 4.4 Writing the End-User Requirement

4.4.1 It is sometimes instructive to see what generic requirements and/or issues have been identified by others who perform a similar task, even if the method is different.

4.4.2 Different units in the same organisation may have subtly different operational requirements – for example, methods for volume crime investigations may have different requirements than in counter-terrorism. This will be reflected in the likely included inputs and constraints (for example, timescales, budget) as well as outputs. If a method is required to be for intelligence the end user is the investigation team, but if the ultimate user of the output is still expected to be the courts then this must be reflected in the requirement.

4.4.3 When developing the end-user requirement, it is often useful to consider if the expected output will be affected by any of the following.

a. Factual – absolutes (for example, the following data were recovered, but other data may have been present).

b. Technically interpreted – where the original output cannot readily be interpreted by a 'layperson'. The competence of the individual interpreting the data must also be included in the assessment.

c. Evaluative – use of a technique to enable an expert to give an opinion on a wider question. The competence of the expert must also be assessed, not only in the use of techniques but on their ability to provide expert opinion.

4.4.4 For example, if the method is to find JPEG [8] images by their file extensions then the requirement may be quite straightforward, as will the associated acceptance criteria and subsequent testing. If the user-requirement is to find all photographs (possibly including those partially overwritten) it becomes quite nuanced. Such an open requirement may require a lot of testing; even then it is likely that commonly encountered files for the types of case expected will need to be specified. If the user-requirement was for types of case that include forgery, then a different set of proprietary image types might also need including.

4.4.5 The end-user requirement needs to be translated into a technical specification of what the method is actually expected to do, and therefore validated to do. There may need to be iteration back with the user who identified the requirement. Continuing the example on images, the technical specification may well need to list the file types it will be expected to find and caveat that proprietary files from photo editing software are excluded. Essentially the user

[8] The acronym relates to the Joint Photographic Experts Group that created this method of lossy compression for digital images.

of the report needs to understand the limitations of the method; if the user understands this then the acceptance criteria can be developed.

4.4.6 The example below from the literature shows increasing technical detail being derived from one high-level end-user requirement; each aspect can be further developed with more granularity to produce a testable specification (particularly once acceptance criteria are added). [6]

> **“Initial high-level customer requirement**
>
> To obtain an appropriately comprehensive and accurate read-out of the information stored on the evidence item.
>
> **Requirement**
>
> a. A complete copy of the persistently stored user-accessible data on the evidence item, as presented at the time of examination by the disk controller using the logical block address scheme, shall be acquired.
>
> b. Areas hidden by the disk controller using widely recognized standard methods (host protected area, device configuration overlay) shall be acquired.
>
> c. Etc.”

4.4.7 All statements of requirements are unique to an organisation or forensic unit, for example an organisation might not require host protected areas or the device configuration overlay to be acquired. Forensic units may look to more generic requirements as a starting point, however, accreditation requires a demonstration of technical competence that is likely to include an ability to explain the rationale of inclusion or omission of requirements, as well as the technical basis for the acceptance criteria.

## 4.5 Method Development

4.5.1 The methods used by organisations that perform digital forensics are referred to in ISO17025 as ‘laboratory-developed methods’. Laboratory-developed methods answer specific, regularly requested needs by combining tools, techniques and expertise unique to the set-up of the laboratory. For instance, acquisition of a bit-by-bit copy of a hard disk drive would be considered to be a laboratory-developed method mainly because the exact method and set-up/configuration of equipment is bespoke. Laboratory in this sense means the organisation, or forensic unit.

4.5.2 Prior to validation, the method needs to be precisely defined. The most appropriate way of doing this is to ensure that there is a standard operating procedure (SOP) prior to starting the validation study. The method should be sufficiently detailed to allow a competent individual to be able to follow and contain any risk mitigation steps and/or quality controls.

4.5.3 If this is the first time the method has been captured in a SOP, then this may be somewhat iterative as method development often feeds from the technical specification derived from the end-user requirement and risk assessment. If this is an adopted method then the method may well be in the form of a SOP already.

4.5.4 The method ought not be a regurgitation of the user manual of any tools contained in the method, and should focus on reproducibility with reference to aspects of the tool used relevant to the user requirement.

4.5.5 A thorough review of the requirements can ensure that all quality control stages are built into the methodology. Often the easiest risk mitigation steps or quality controls are manual checks and verifications. Checking hash values is a common manual check that is included in a method; they are there to control a risk and if correctly included in the method avoid complicated testing and validation of technical solutions to the same problem. The effectiveness of these will need to be assessed against the risk analysis and the user requirement. The level of testing before the method is deployed is dependent on the complexity of the control so it is preferable at the method development stage to design simple, yet effective, controls.

4.5.6 It is often necessary to transfer learning from a successful validation study to the final SOP. At the simplest level this is taking into account any caveats about the assessment of uncertainty that should be reported with the result of an examination. However, if the validation prompts any change to the method or configuration of the system, there is a requirement to risk assess and verify that the change has not adversely influenced the fitness of purpose. Significant changes may prompt re-validation of the methodology and tools used along with an update of the SOP.

## 5. Risk Assessment

5.1.1 An appropriate and balanced risk assessment is at the core of any validation study, and should concentrate on realistic risks and not become an abstract 'what if' process.

5.1.2 Each risk assessment needs to be particular to the forensic unit; it cannot be an entirely generic approach. Risks will differ as varying equipment and software tools are used and different environmental conditions prevail. Risk assessment in the CJS often includes the:

a. Risk of wrongful conviction(s);
b. Risk of wrongful acquittal(s); and
c. Risk of obstructing or delaying investigation(s).

5.1.3 It is important to know how a method or tool is to be used and, also important, how they may provide misleading results in certain circumstances. The following summarises some of the sources of potential misleading results. [7]

a. Incompleteness – the inability to recover or find all the data.
b. Inaccuracy:
   i. Existence – do all artefacts reported as present actually exist?
   ii. Alteration – does a method alter data in a way that changes the meaning, such as updating an existing date-time stamp (for example, associated with a file or email message) to the current date?
   iii. Association – for every set of items identified by a given method, is each item truly a part of that set?
   iv. Corruption – does the forensic method detect and compensate for missing and corrupted data (including, where relevant, any deliberate editing or manipulation prior to receipt)?
c. Misinterpretation.

5.1.4 From the above list the most common in many of the digital forensic applications is likely to be incompleteness. Incompleteness is less likely to increase the risk of wrongful conviction, but it might prevent effective investigation and/or delay justice for victims. For this reason it is important that the forensic unit understands any limitations of the method and discloses them appropriately to the end user. A requirement for a method to find every fragment of data possible in a terrorism case might be proportionate, but if it was expected in every case it could create long delays in casework. It could also create its own risk of some cases being turned away from having any digital examination due to the resource implications.

5.1.5 Should inaccuracy or misinterpretation occur the impact is more visible. Occasionally the courts do encounter such issues, but case law rarely comments on the inability to find evidence as the case is less likely to have been put before them. The impact of incomplete data should be considered, and the risk proportionately mitigated against.

5.1.6 A thorough understanding of the method, technique and technology should allow practitioners to identify the type of error that could occur at any stage in the series of tasks in the method, and the validation can assess the mitigation.

5.1.7 For example, during the examination of almost any digital exhibit there is the possibility of altering data on that exhibit by writing data to that device. This is typically mitigated by the use of hardware or software write-blocking, to prevent writing to the device. In some instances, write protection at the binary level is not possible, such as in the examination of mobile telephones [9] or encrypted systems that need to be powered on and live to allow access to the device. In instances such as these, the risk of altering the data likely to be of interest needs to be assessed and managed.

5.1.8 In certain parts of the process, the use of visual/manual checks could be demonstrated to mitigate the identified risks in the method. The risk might not be that a method might not work; it could be not being able to tell if it worked or not (for example, a file search). Here, the ‘avoid’, ‘reduce’ or ‘accept’ responses in traditional risk assessment processes used in project management are often

[9] The majority of mobile phone forensic software has write-protect data at the logical, extant, level.

used. Here, risks that cannot be mitigated or corrected within the total method may be accepted as caveats to the results reported, if the acceptance criteria allow. However, this does need a firm and balanced understanding of what that acceptance means. For example, the investigation team may accept that not all evidence is recovered, provided most is. Unfortunately, the unrecovered data may not be only inculpatory evidence, the data could be exculpatory and therefore this risk needs to be managed also. For this reason, methodologies used in project management which guide the assessor toward prompts such as accepting or transferring the risk, might not be ideal for looking at mitigation for risks to the CJS.

5.1.9 An alternative to traditional risk assessment processes used in project management, are ones such as failure modes and effects analysis (FMEA). [8] Process FMEA is one of a number of similar methods best used with process mapping; it looks at each step in the method under assessment and prompts the assessor to describe what could go wrong, how this failure will affect the function of that step, give an indication of the root cause(s) or reason for the failure and what controls are currently in place to catch, detect or prevent this failure. This does not prompt assessors to 'accept', it focuses on detecting issues and the operation of controls.

5.1.10 Whichever risk assessment method is used, it is good practice to cross reference between the risk within the risk assessment table and the stage in the procedure that mitigates or controls that risk. Identifying what controls are to be assessed during validation, and which have an alternative assurance mechanism, ensures the testing is focussed. Clearly if training is considered the mitigation of for an aspect of the operation of the method, it would seem reasonable that it can be demonstrated that the training material specifically covers the issue at hand.

5.1.11 This proper consideration of the nature of risks feeds into the validation strategy, highlights specific tests that might be required and influences the scale of the validation.

# 6. Scale of Validation Required

## 6.1 Introduction

6.1.1 The scale of validation exercise will vary according to:

a. The complexity or novelty of a method;

b. The data that are available from previous studies, evaluations or validations;

c. The risk assessment; and

d. What the end user actually requires the method to do.

6.1.2 Defining the specific purpose from the onset, focusing on starting with the most common functionality and requests, should prevent the scope of the validation study creeping into attempting to cover everything the method might be used for, which is not practical or realistic. Once the purpose, or user requirement, is complete objective evidence can be delivered through various routes.

6.1.3 Keeping in mind that the validation is about the method, the various types of validation studies tend to fall in the following range.

a. A new or novel method will require comprehensive testing. This will include the assessment of both the equipment or software and the approach taken when using it in order to provide assurance that it is fit for purpose. If the method or validation approach is sufficiently novel, it may be beneficial for a version of the validation report to be submitted for publication in a journal.

b. An adopted method, which was originally validated elsewhere and where the data are available, will require a critical review of validation records to ensure:

   i. That the validation performed is fit for purpose; and

   ii. Verification that the laboratory is competent to perform the test/examination, i.e. it works in their hands.

c. An update to a method (for example, new equipment, software version) that has already undergone validation within the organisation will require a risk assessment, targeting and usually testing the specific changes. If the risk assessment or testing determines that the change is significant then it may need full re-validation.

6.1.4 These three scenarios are complicated by the fact that many methods may have been in use for a while but there are no or little available validation data. With a reduced data set to review, some organisations may be pushed into treating what they might consider routine methods as novel, which require comprehensive testing. The digital forensics community is free to collaborate on aspects of the validation study. This is a mix of the approach required for novel methods in Section 6.2 below, with each individual organisation then evaluating the aspects of validation study performed by the collaborating third parties as covered in Section 6.3.

6.1.5 Where an organisation is deemed competent to perform the tests it should be competent to understand what type of objective evidence would be required to demonstrate the validity of the method used.

## 6.2 Novel Methods

6.2.1 If a method has been used in the digital forensics community for a while but has no relevant and reliable validation data supporting it, or is entirely novel, then the validation required is often termed a developmental validation. This is in contrast to an internal validation of a method adapted or adopted from elsewhere. A developmental validation will require much more testing as there is no objective evidence of it being fit for purpose to evaluate. Methods adopted/adapted from elsewhere where pre-existing validation data are available is discussed in Section 6.3.

6.2.2 Validation needs to show that the method is fit for its purpose as well as managing risk. The risk assessment (see Section 6) of the specification developed from the user requirement should focus validation activity on what will make a difference to critical findings. However, with a truly novel method it is possible that none of the functional requirements have been properly assessed and any or all features that the method will rely on may need an element of stress testing. A working understanding of experimental design is essential when validating novel methods; a well designed test can maximise the utility of each element of the test and ensure that the amount of testing is kept to the minimum required to achieve confidence in the fitness of purpose.

6.2.3 Consideration of whether scripts written by the forensic unit to aid in the extraction and presentation of data are novel is somewhat subjective. However, they do require validation. If a forensic unit is regularly generating such scripts then having a script development, testing and validation protocol should allow that appropriate scaling of testing occurs.

6.2.4 A novel method using new software tools will include the sort of validation and verification procedures dictated in software engineering to demonstrate that the software development was to the required standard. Appropriate standards ensure that the software's internal engineering is correct. Therefore, there should be evidence of use of a formal development method and/or a quality management systems, as well as evidence of unit and system testing, including test plans and results.

6.2.5 Even software developed within a suitable quality standards framework may only be as good as the technical or functional specification supplied. Omissions or errors that occur in the functional specification will be faithfully coded into the software and even if handed over to independent software testers, may still pass the test.

6.2.6 Software that is deemed valid in software engineering terms forms part of a wider method. The overall method will then need testing in more of a black box [10] following the steps detailed in this document, as well as the Codes.

6.2.7 Whether a method is truly novel is a little subjective. Even if the novelty of the method is self-evident or if a method is deemed novel simply because it utilises a bespoke software tool then Section 6.3 may well assist, once the software testing requirements are fulfilled.

6.2.8 The end goal is that the implementing organisation has similar objective evidence available whether it developed or adopted/adapted the method. The difference with a truly novel method is the amount of data generated by the

[10] A method of testing functionality using inputs with known (or expected) outcomes without requiring knowledge of the internal structures or coding of the application.

implementing organisation is much greater, although the plus side is if this is a novel capability it may well be in great demand.

## 6.3 Adopted and Adapted Methods

6.3.1 The requirement is to be able to produce objective evidence that the method is valid. ILAC-G19:08/2014 expands on the point stating:

> "When a method has been validated in another organization the forensic unit shall review validation records to ensure that the validation performed was fit for purpose. It is then possible for the forensic unit to only undertake verification for the method to demonstrate that the unit is competent to perform the test/examination." (Section 3.10 of ILAC-G19:08) [4]

6.3.2 The above description is often referred to as verification; in reality it is performance verification with a key proviso that the validation records have been reviewed first. To review the existing validation records implies that:

a. There is something to review the validation records against (i.e. an end-user requirement and technical specification);

b. There is access to the validation records in sufficient detail to assess against the end-user requirement, specification and risk assessment; and

c. The method is the same or demonstrably comparable.

6.3.3 Most fields in forensic science use some form of adopted methodology where some or all of the validation data are available elsewhere. As previously stated in paragraph 6.3.1, if another organisation has validated a method, complete re-validation may not be necessary. However, the method will require reviewing to see that it is fit for purpose based on the available data. If the existing data do not cover the entire new requirement then the gaps in the objective evidence will need to be filled. However, if the data are deemed inadequate, unreliable or simply unavailable, then a complete validation will need to be carried out as if the method was novel.

6.3.4 Before verification is performed to show that the forensic unit is competent to perform the test/examination, the forensic unit must review/assess/verify that the external/developmental validation:

a. Was relevant to the way that the method is intended to be used; and

b. Had been conducted in a scientifically robust manner.

6.3.5 A working understanding of experimental design is essential when validating new methods, but also important when assessing external validation data of the method being adopted or adapted.

6.3.6 Assessing the relevance and completeness of objective evidence produced by others in collaborative or developmental validation studies should be relatively straightforward. If the requirements laid out in the Codes for each of the steps of the validation process have been completed, differences in the user requirements and methods are more likely to be visible.

6.3.7 The Regulator’s more general guidance document on validation (FSR-G-201) gives more detail on evaluating the reliability of externally derived objective evidence.

6.3.8 Detailed evaluations of tools used in a method such as produced in the USA by the National Institute of Standards and Technology [9] can be of great assistance but do not replace the need for validation; if a manufacturer or supplier of tools provides data these also can be objectively evaluated within the overall user-requirement of the method.

6.3.9 When a method is shown to be fit for purpose largely through a review of validation records produced by anyone other than the forensic unit’s own competent staff, there is still a requirement to produce objective evidence that the forensic unit can perform the method.

6.3.10 Therefore, verification in the context used in assessment to ISO17025 can be thought of as demonstrating that:

a. The existing objective evidence produced externally is relevant, available and adequate for the intended specific purpose, and that a method performs reliably and validly at the given location with the forensic unit’s own staff; or

b. A method remains fit for the specific purpose following a minor change in the process, and if the change does not require revalidation of the method.

6.3.11 The Codes require this check to be against the required specification for the specific use for which a method is being employed, rather than simply against existing published data.

## 6.4 Minor Changes

6.4.1 Replacing like-for-like equipment or minor changes to methods used by the forensic unit will not always require a full revalidation exercise, but it will require some recorded activity. A risk or impact assessment is required, which should be focused on what changes have occurred and compare these with the original validation. It might be that new functionality has been included as well as updates to existing capability. The changes may be within the tolerance of the original acceptance criteria or the existing quality assurance methods built into the method may be quite capable mitigating against identified risks.

6.4.2 The criteria for the assessment of impact or risk as to whether the change would or would not prompt a re-validation should be taken from the original validation study; this should allow any changes that might adversely affect the operation or validity of the critical findings to be identified and checked. The key to assessing the change is a thorough understanding of the technique, the original validation, the acceptance criteria, risk assessment and relationship of upstream and downstream activities.

6.4.3 Small changes in a method such as a software version update, for instance, may change the output format. This may impact on any of the subsequent or upstream activities (and not always just the one immediately upstream). Changes that are being considered because they enhance the process in some way, or correct for a previous bug, may also have unintended consequences.

6.4.4 All methods will have some level of quality assurance stages, quality checks and/or even reality checks by an expert, which control the risks associated with that specific part of the method or the entire method. If these checks are well designed and well tested, then a degree of robustness or ability to accommodate specific changes may have already been tested. Almost all acceptance criteria will have a range of tolerances methods where certain changes are anticipated. The acceptance criteria may well have specified how to assess small changes that are required, or even have this included in a change control or method modification protocol.

6.4.5 Unmanaged changes can add unnecessary risk, may invalidate the procedure and/or the associated accreditation. Great care should be taken if the changes are not within the parameters of an approved change control or method modification protocol.

6.4.6 If the method must be operated outside of accreditation for a specific application, then this must be made clear to the customer. The Criminal Practice Directions discussed in Section 4.3.1 will still apply, which require the disclosure of the validation status. Thankfully, the risk-based assessment that may have demonstrated that the method no longer meets the original acceptance criteria, may also offer a new estimate of uncertainty resulting from this change. This may mean that the court can still adequately evaluate the findings. If the now new method is to become part of the routine activities of the forensic unit, accreditation should always be sought.

6.4.7 Accreditation is about demonstrating competence. This can be taken to include the ability to assess correctly minor changes to methods. The above guidance should give an insight into how procedures will be developed, but ultimately it is for the organisation to demonstrate that it has a sufficient understanding of how changes may impact the results.

# 7. Validation Requirements and Acceptance Criteria

## 7.1 Introduction

7.1.1 The validation requirements of a given method will include the tools employed, the risks and the output required. These should be defined at the outset of any validation testing, and should highlight the following.

7.1.2 Any aspects of the method that directly impact the results or critical findings.

7.1.3 Aspects of the method that have lesser importance but may also be tested and assessed.

7.1.4 Any issues expected (including any mitigation of these issues).

7.1.5 These issues need to be realistic issues and not theoretical in the abstract.

7.1.6 A validation will take the form of one or more tests of each of the specified requirements. A single test of a method in and of itself does not mean that a method is validated. Robust testing methods are required, employing as many tests as necessary to demonstrate fitness of purpose. The validation plan should be based on good experimental design to ensure that the testing is scaled and targeted correctly.

7.1.7 For example, the testing of hardware write blocker can be achieved simply within a Windows environment by attempting to write data to the drive. However, if this it to be used with other operating systems such as Linux then this would also need to be tested.

7.1.8 The validation should include the full range of activity required of the method and include acceptance criteria.

## 7.2 Validation Strategy and Plan

7.2.1 Once the requirements are defined, they should be used to inform the approach taken for validation (i.e. the strategy). The strategy is an overview of the whole validation process and forms an outline of the plan**.** The plan is a series of discrete, achievable and measurable steps, each part of the process defining the specifics of the data used and the expected outcome. The strategy/plan should define the following.

a. Method under review.

   i. This should include all relevant details including the manufacturer of tools included, versions of hardware, firmware and software and the version number of the method's standard operating procedure.

b. Type of result being assessed.

   i. Whether the method is, for example, factual, technically interpreted or opinion.
   ii. A technically interpreted method will probably also require an assessment of the validity of the factual output of equipment.
   iii. Likewise, when a method encompasses opinion, the technical interpretation and factual outputs that form parts of the overall process may also require assessment.

c. Source, quantity and reliability of data used for the tests.

   i. If data recovery assessments are being performed, a review of the source and type of data used should be undertaken; this should include whether the data are likely to provide problems for the system being assessed (i.e. whether the data enable a 'stress test'). For example, this could include non-standard character sets, formats, file locations or volumes of data.

ii. If measurements involving standard units are being performed, the provenance and accuracy of the source (the traceable standard) should be established.

iii. If technical interpretation or opinion assessments are being performed, blind trials may be used in addition to the other tests.

iv. Blind trials should focus on non-obvious situations where a failure to assess correctly is a real prospect.

v. If there is little or no control of the source data, this should be explicitly declared in the plan and the subsequent limitation declared.

d. The expected outcome for the tests performed, to include consequences or next steps if the expectations are not met. Expected outcomes should be, wherever possible, specific, quantifiable and highlight the acceptable error margin (i.e. the defined accuracy and precision required of the method).

e. Limitations of the tests performed. For example, a limited data set has been used, or the data may potentially change with time.

## 7.3 Assessing Uncertainty in Digital Forensic Science

7.3.1 Assessing uncertainty is often best addressed in the validation study and is an ISO17025 requirement. Uncertainty may be presented in terms of a false positive or negative (see Section 5 on risk assessment) or in terms of accuracy and precision.

7.3.2 Precision is synonymous with reproducibility or repeatability, whereas accuracy is the closeness to the true or correct value for the quantity measured. For instance, a timestamp is precise (for example, 03/03/2015 11:48:08) but precision does not automatically convey accuracy. The method would employ a number of ways of estimating and controlling the impact that uncertainty might have on any inferences made from a timestamp. The requirement is to ensure that if uncertainty remains, the form of reporting correctly conveys this underlying uncertainty to ensure that the user of the information is not misled.

7.3.3 In a search by file extensions for images, a factual report may state that precisely x number of files were found; uncertainty may remain about how many images were actually present on the media searched. This caveat might be entirely acceptable and understood for one application. For others the method would employ other searches to increase the level of confidence that the majority of files present would be found. Acceptance criteria that demand 100 per cent in anything other than a data set designed for evaluating a method should not be agreed to. Likewise, if there is always a possibility that some files might still not have been found, an appropriate caveat is often all that is required.

7.3.4 Where the results of the test are neither numerical or measurement based, the requirement is that as many components of uncertainty are identified, their impact assessed, and attempts made to mitigate their influence (for example, tighter controls in procedures, uses of multiple tools, introduction of checks). If the uncertainty has an effect on the reliability of the output and there is no mitigation, then it needs to be reported with the results.

## 7.4 Generation and Control of Test Data

7.4.1 The design of the test is dictated by end-user requirements and technical specifications, along with any relevant risk assessment.

7.4.2 If the method being tested is an adopted method, then the design of the test used to create the validation data must be critically assessed. If the design was inadequate or not relevant to the proposed implementation of the method, then the validation study must be performed to demonstrate that it is fit for purpose.

7.4.3 Understanding the scale of the validation study undertaken is crucial in selecting the representative data required. This section also should give an insight into the required features of the data that should be looked at in the assessment. If this is a verification of an existing adopted method validation study, the same standard needs to be achieved.

7.4.4 For example, a search or data recovery method may require bulk known data to access for testing purposes. These data should include the following wherever practicable or relevant.

a. Representative data types that the method is expected to work on.
b. Where data or character types are known to have caused problems in similar methods, the test data should include such data to provide this type of stress test.
c. The quantity of data should be adequate to provide a rigorous test of the process.

7.4.5 It is not always possible to define the source data completely. However, every effort should be made to select data that will robustly test the method and tool to be used.

7.4.6 Data created for and generated during the validation should be stored for later audit.

## 7.5 Undertaking Validation

7.5.1 Once the requirements, strategy and plan have been defined the tests can be performed.

7.5.2 As with most activities in forensic science, contemporaneous notes are required to be taken and for each test in the plan, should detail:

a. Who undertook the test;
b. When the test took place;
c. What the test assessed;
d. What equipment was used;
e. Where the test was performed;
f. The expected outcome; and
g. What the results were.

## 7.6 Evaluation

7.6.1 Each test in the plan should be carried out and the result compared with the expected outcome (i.e. the actual result versus the expected or acceptable outcome). An assessment should be made as to whether the method has passed or failed each of the tests, and is fit for purpose.

7.6.2 Testing should not normally be limited to a single event. There should be a consideration of uncertainty of measurement that usually is achieved by repeating tests. These can include:

a. Duplicate equipment, run on the same data in the same environment at the same time or, if relevant, calibrated in the same manner;
b. The same equipment on the same data in the same environment at different times;
c. Checks for bleed through of data from previous searches (for example, performing a search on large data set followed by a search on smaller data set); and
d. Where the method needs to be portable (for example, to be used at scenes of crime) validation should include a robustness test to evaluate its operation under different circumstances.

7.6.3 If the plan has to change at any point during the study, the impact this has on the utility of the study should have been assessed and recorded. This includes instances where the discussion to change was supported by the other stakeholders/end users involved in developing the user requirement and plan.

7.6.4 Within the contemporaneous notes, the findings should be summarised to include the following.

a. The original requirement for each test and a summary of the findings.
b. Whether the method meets the original requirement:
    i. Any areas in which the method fails to meet the requirement should be explicitly highlighted;
    ii. Any limitations of the validation approach and the method itself should be detailed.

7.6.5 If a method fails an individual test, in consultation with the other stakeholders/end users it may be possible to recommend:

a. a re-assessment of whether the specific capability that failed the test is mandatory or desirable (i.e. whether the failure of the aspect tested should result in the entire method being discredited);

b. inclusion of additional quality checks to detect or mitigate the failure; [11]

c. a method change and a new validation study.

# 8. Concluding Validation

## 8.1 Validation Report

8.1.1 A report should be constructed that details the validation process performed. This should include the following:

a. The original requirement;

b. Reference to what is, and is not, validated;

c. A summary of the strategy, tests performed and the outcome of each test;

d. Reference to the data used and any limitations accepted from the onset these may have on the tests performed and therefore what caveats apply;

e. Whether the method is fit for purpose – this should state whether the method is fully approved, partially accepted or not recommended for use;

f. A caveat to suggest that reliability and uncertainty measures have been considered and what impact these may have should be included.

g. Recommendations for use:

   i. To include any limitations of the method, the impact of these limitations, and any additional steps required to detect and mitigate for them;

   ii. To define the required ongoing quality regimen (for example, quality assurance tests); and

   iii. To explain the effect of this new validation on other methods previously used to this purpose, i.e. whether the other method becomes obsolete and should be superseded, or if it can be used as an alternative or in parallel.

[11] Changes to the method itself may have unintended consequences and prompt a new validation study, whereas as an additional manual quality check may be assessed as acceptable.

## 8.2 Statement or Certificate of Validation Completion

8.2.1 The Codes require that a statement or certificate of validation completion be produced by the organisation implementing the method. A statement from a third party that the method is valid is not an acceptable alternative. All that is required is a short (one or two page) summary of the validation report. The assumption is that the certificate is essentially recording approval, although it could record that the method is not recommended for use.

8.2.2 The approver should be suitably senior in the organisation and demonstrate adequate objectivity and/or independence from those undertaking the validation study. Refer to section 20.15 of the Codes for further details.

## 8.3 Implementation

8.3.1 Once a method has passed validation and is approved for use, there will be further activities required before it can be used on live casework. These activities should include the following.

a. Training plan for users, including the competency requirements and testing.

b. Guidance for use, including defining ongoing quality assurance.

c. Inclusion in existing systems (for example, equipment logs, competency records, quality system).

# 9. Post-Validation Activities

## 9.1 Maintenance of Records

9.1.1 Reference to the validation may be included in quality documentation and the report should be included in the validation library held by the organisation performing the validation. There may also be links to other requirements that are not directly concerned with validation, for example, equipment logs detailing changes in use. The validation records are required for as long as the records of the cases they were used on; for example, they may be required later in an appeal court.

## 9.2 Quality Assurance

9.2.1 Ongoing performance testing is recommended to monitor performance drift. The results should be recorded in the training and/or equipment documentation.

## 9.3 Acceptance Testing of New Equipment

9.3.1 If new equipment of the same design (manufacturer, version, firmware) is purchased, an acceptance test may be in the form of a configuration check to form part of the equipment log.

# 10. Review

10.1.1 This document is subject to review at regular intervals.

10.1.2 If you have any comments please send them to the address or email set out on the Internet at: www.gov.uk/government/organisations/forensic-science-regulator.

# 11. References

[1] Ministry of Justice, "What's New? Criminal Procedure Rules," [Online]. Available: www.justice.gov.uk/courts/procedure-rules/criminal. [Accessed 31 07 2020].

[2] International Organization for Standardization, Conformity assessment — Requirements for the operation of various types of bodies performing inspection, ISO/IEC 17020:2012.

[3] International Organization for Standardization, General requirements for the competence of testing and calibration laboratories, BS EN ISO/IEC17025:2017.

[4] International Laboratory Accreditation Cooperation, "Modules in a Forensic Science Process, ILAC G19:08/2014," [Online]. Available:

https://ilac.org/latest_ilac_news/ilac-g19082014-published/. [Accessed 31 07 2020].

[5] “Legal Obligations,” [Online]. Available: www.gov.uk/government/collections/fsr-legal-guidance. [Accessed 31 07 2020].

[6] European Network of Forensic Science Institutes, “Best Practice Manual for the Forensic Examination of Digital Technology, ENFSI-BPM-FIT-01,” [Online]. Available: http://enfsi.eu/wp-content/uploads/2016/09/1._forensic_examination_of_digital_technology_0.pdf. [Accessed 31 07 2020].

[7] Scientific Working Group on Digital Evidence, “Establishing Confidence in Digital Forensic Results by Error Mitigation Analysis Version: 1.5,” [Online]. Available: www.swgde.org/documents/Current%20Documents. [Accessed 31 07 2020].

[8] Forensic Science Regulator, “Validation,” [Online]. Available: www.gov.uk/government/collections/forensic-science-providers-codes-of-practice-and-conduct. [Accessed 01 08 2020].

[9] National Institute of Standards and Technology, “Computer Forensics Tool Testing Program (CFTT),” [Online]. Available: www.cftt.nist.gov/. [Accessed 31 07 2020].

# 12. Glossary and Acronyms

**Accreditation**

Third-party attestation related to a conformity assessment body conveying a formal demonstration of the forensic unit's competence to carry out specific conformity assessment tasks.

**Accuracy**

The closeness of agreement between the mean of a set of results or an individual result and the value that is accepted as the true or correct value for the quantity measured (see also precision).

**Calibration**

The set of operations that establish, under specified conditions, the relationship between values indicated by a measuring instrument or measuring system, or values represented by a material measure, and the corresponding known values of a measurand.

**[The] Codes**

The Codes of Practice and Conduct for Forensic Science Providers and Practitioners in the Criminal Justice System, published by the Forensic Science Regulator.

**Competence**

The skills, knowledge and understanding required to carry out a role, evidenced consistently over time through performance in the workplace. The ability to apply knowledge and skills to achieve intended results.

**Contamination**

The undesirable introduction of substances, trace materials or data.

**Criminal Justice System**

The Criminal Justice System (CJS) is the collective term used in England and Wales for the police, the Crown Prosecution Service, the courts, prisons and probation, which work together to deliver criminal justice.

**Critical findings**

Typically observations or results that meet one or more of the following criteria.

a. Have a significant impact on the conclusion reached and the interpretation and opinion provided.

b. Cannot be repeated or checked in the absence of the exhibit or sample.

c. Could be interpreted differently.

**Customer**

Whether internal or external, it is the organisation or the person who receives a product or service (for example, the consumer, end user, investigating officers, defence, prosecution, retailer, beneficiary or purchaser).

**Databases**

Collections of information designed to provide information rather than for archive, which are stored systematically for later retrieval or searching in hard copy or electronic format and are, for example, used for:

a. Providing information on the possible origin of objects or substances found in casework; and/or

b. Providing statistical information.

**End user**

The end user of forensic science is the Criminal Justice System, essentially the courts. A method or tool may not be directly used by the courts, but it is assumed that the results will be.

Anything that may prove or disprove an assumption to be true, for example, an exhibit or the lack of expected findings.

**Expert (witness)**

An appropriately qualified and/or experienced person familiar with the testing, evaluation and interpretation of test or examination results, and recognised by the court to provide live testimony to the court in the form of admissible hearsay evidence.

**False positive/false negative**

A false positive is the inclusion of a result that is incorrect in an output. A false negative is the exclusion of a correct result from an output.

**FEMA**

Failure Mode Effect Analysis.

**Fit for Purpose**

Good enough to do the job it is intended to do, as defined by the specification developed from the end-user requirement.

**Forensic unit**

A term used in ILAC-G19 to mean "a legal entity or a defined part of a legal entity that performs any part of the forensic science process". It is interchangeable with provider. However, it is used in this document as these are small teams or sole practitioners that for accreditation purposes may be considered separate legal entities in larger organisations, FSPs and police forces.

**Intelligence**

Intelligence is information transformed through an analytical process.

**JPEG**

A method of lossy compression for digital images named after the Joint Photographic Experts Group, which created it.

**Measurand**

A physical quantity, property, or condition quantity that is being determined by measurement.

**Method**

A logical sequence of operations, described generically for analysis or for comparison of items to establish their origin or authenticity.

**Method validation**

The process of verifying that a method is fit for purpose (i.e. for use in solving a particular problem).

**Organisation**

A group of people and facilities with an arrangement of responsibilities, authorities and relationships (for example, a company, corporation, firm, institution, charity, sole trader, association, or parts or combination thereof).

**Precision**

Precision is synonymous with reproducibility or repeatability. An incorrectly calibrated device may be capable of giving reproducibly precise readings even though data generated are not accurate.

**Provider**

The term ‘provider’ is used to include all providers of forensic science, whether commercial, public sector or internal to the police (for example, scenes of crime, fingerprint bureau). See also forensic unit.

**Qualitative**

Results or requirements based on some quality rather than on some quantity, i.e. the identity of the compound rather than concentration.

**Quality**

The totality of features and characteristics of a product or service that bear on its ability to satisfy stated or implied needs.

**Quantitative**

A measurement or requirement based on some quantity or number.

**Risk**

The probability that something might happen and its effect(s) on the achievement of objectives.

**Robustness**

The capacity of an analytical procedure to remain unaffected by small, but deliberate, variations in method parameters.

**SOP**

Standard Operating Procedures

### Standard methods

A 'standard method' is published by certain prescribed organisations and has the following characteristics:

a. Contains concise information on how to perform the tests;

b. Does not need to be supplemented or rewritten as internal procedures; and

c. Can be used as published by the operating staff in a laboratory.

Based on the full definition in ISO17025, at the time of writing (2020) there appear to be no 'standard methods' in the forensic sciences in the UK.

### Stress testing

A data set used in validation specifically designed to expose expected or reasonable deficiencies of the method under test.

### Uncertainty of measurement

The estimation of the uncertainty of measurement is an ISO17025 requirement. It is based on the principle that all measurements are subject to uncertainty and that a value is incomplete without a statement of accuracy. Sources of uncertainty can include unrepresentative samples, rounding errors, approximations and inadequate knowledge of the effect of external factors.

### USB

Universal serial bus – technology for connecting devices to a computer.

### Validation

The process of providing objective evidence that a method, process or device is fit for the specific purpose intended.

### Verification

The context that is used in the accreditation assessment is best described in ILAC-G19:08/2014 (3.10) where it refers to verification thus:

"When a method has been validated in another organization the forensic unit shall review validation records to ensure that the validation performed was fit for purpose. It is then possible for the forensic unit to only undertake verification for the method to demonstrate that the unit is competent to perform the test/examination."

Published by:

The Forensic Science Regulator

5 St Philip's Place

Colmore Row

Birmingham

B3 2PW

www.gov.uk/government/organisations/forensic-science-regulator