Forensic Science Regulator
Overseeing Quality

Draft Guidance: Digital Forensics Method Validation

FSR-G-218

Second consultation

This is a consultation draft and therefore should not be regarded or used as a standard. This draft is issued to allow comments from interested parties; all comments will be given consideration prior to publication, the consultation will run from 18 December 2015 to 5 February 2016. Comments should be sent to FSRConsultation4@homeoffice.gsi.gov.uk using the form available from https://www.gov.uk/government/organisations/forensic-science-regulator and should be submitted by 5 February 2016. This mailbox is not for general correspondence and is not routinely monitored so no acknowledgement will normally be sent.

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 and have a very reasonable expectation can 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. Top of the list the Criminal Practice Directions[1] suggest the court take into account when determining the reliability of expert opinion is:

> *"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 accreditation to the international standard ISO17025,[2] it includes the assessment by a third party that the organisation has demonstrated the methods they use are valid and they are competent to perform them.

1.1.4 Validation is a demonstration of fitness for purpose, the first step is to define what the user of the method and results need it to reliably do. Validations that skip this step may miss the key quality issues, focus on usability alone and can result in unfocussed testing and amassing of data which may or may not increase understanding or give justifiable confidence in the method.

[1] Accessed 24/11/15: https://www.judiciary.gov.uk/publications/criminal-practice-directions-2015/

[2] BS EN ISO/IEC17025:2005 - General requirements for the competence of testing and calibration laboratories.

1.1.5 Most methods are not entirely new so for methods adopted/adapted from elsewhere where pre-existing validation data is available the requirement[3] 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."*

1.1.6 Truly novel methods, or methods which have no pre-existing 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 7.3).

1.1.7 With the exception of methods which are almost entirely tool operation (e.g. a simple USB acquisition tool), most methods will have quality assurance stages, 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.

1.1.8 The validation requirements of a given method will depend on the tools employed, the risks and the output required. 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 If conducting a validation on a method that has not been tested before, bulk known data is likely to be required. Data for all validation studies has

[3] 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.

to be representative of the real life use of the method will be put to, but it has not been tested before it will also need to include data challenges which can **stress test** the method.

1.1.10 If the method being implemented is an adopted method purporting to have been validated by another organisation, part of review on their validation study data includes whether the selected in the original validation did indeed robustly test the method and tools in a manner that matches your 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 user of the method to demonstrate validation, although the developer may greatly assist the end user by providing information on the testing they have performed.

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 case work, too complex, 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 extensive the data set.

2 INTRODUCTION

2.1 Purpose

2.1.1 The courts have the expectation that the methods that produce the data that a expert bases their opinion on are valid.[4] Validation is the recognised way of demonstrating this, and method validation is a key requirement for accreditation to the ISO standard BS EN ISO/IEC17025:2005 (referred from here as simply ISO17025). Validation involves demonstrating that the method is fit for the specific purpose

[4] E.g. see the Criminal Practice Directions as amended.

intended, and any limitations are understood and explained. Validation is a central feature of the Forensic Science Regulator's Codes of Practice and Conduct (the Codes), 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 be taken to be the process by which information is extracted from data storage media (e.g. devices, remote storage and systems associated with computing, imaging, video, audio, satellite navigation, communications), rendered into a useable form, processed and interpreted for the purpose of obtaining intelligence for use in investigations, or evidence for use in criminal proceedings. 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 Implementation

2.4.1 This guidance is available from the date of publication to assist organisations in designing and planning validation. This however is a consultation draft and therefore should not be regarded or used as a standard.

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.

3.1.2 Any method in science or engineering can be documented; the creation of a draft standard operating procedure is normal 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 in the end-user requirement.*

3.2.2 The end-user requirement is focussed on in more detail in section 4, at its most simple level, it is capturing what the different users of the method and, as importantly, the results require. A simple method may have a short requirement with only a few factors that that influence the generation of the results, if this is a truly novel method featuring user developed software it 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 and collate the remainder from other sources such as scientific literature or other studies. The requirement is for data to be available that can be evaluated against the implementing organisation's end-user requirement.

3.4 Summary of the Validation Process

3.4.1 Although there may be a number of novel approaches or tools employed within a method, generally most methods are assumed to be at least in part adopted and/or adapted methods rather than truly novel.

3.4.2 Much of this guidance document is written with the assumption that adopted and/or adapted methods are the main methods employed by forensic science providers and more detail is given in section 7.3. However, if there is no reliable pre-existing data on the method, even if it has been in use for some time, then the method may need to be

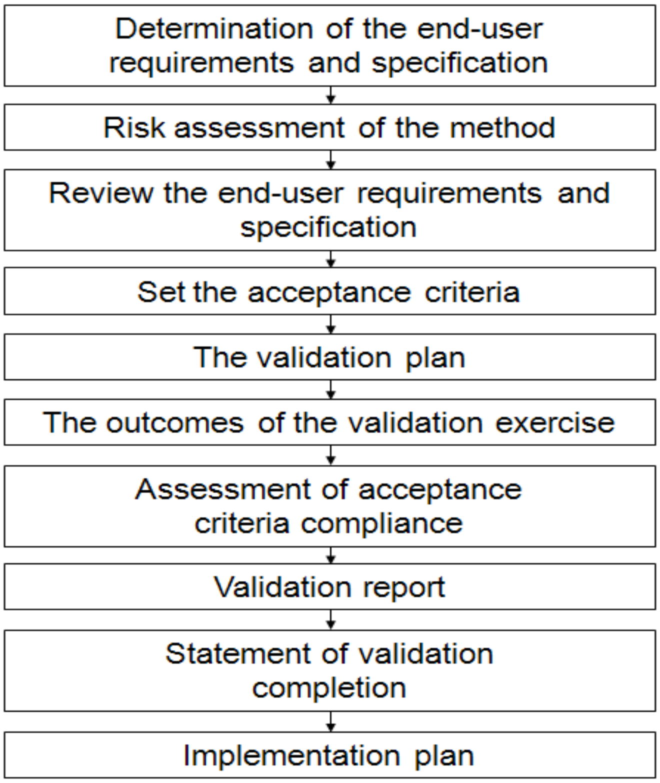

Determination of the end-user requirements and specification
Risk assessment of the method
Review the end-user requirements and specification
Set the acceptance criteria
The validation plan
The outcomes of the validation exercise
Assessment of acceptance criteria compliance
Validation report
Statement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

Figure 1: Framework published in the Codes

treated more as if it was novel as in section 7.2.

3.4.3 Whether the method is novel or in common use elsewhere, the same stages are expected to be followed and sufficient records and paperwork compiled. Section 7.3 describes how some of this may be reviewing the work or others, but the requirement is for the organisation to be able to demonstrate the method is valid and this can only really be done if the organisation can produce appropriately comprehensive evidence to that effect.

3.4.4 Figure 1 shows the stages starting at determining the end-user requirement through to a statement of validation completion and an implementation plan. Following a defined process and compiling the paperwork is required by the Codes, whether conducting a validation study or verifying that validation studies conducted elsewhere are applicable. In simple methods the paperwork produced could be quite short, however the total validation study paperwork should include any external objective evidence used to support 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, and the user of any information derived from it, to be confident about whether the method is fit for purpose as well as understanding any limitations. The requirement to assess if a method is fit for purpose depends upon first defining what the user 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. need 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 which, 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, it 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, laboratories 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 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 upon by other bodies within the Criminal Justice System and must also meet their requirements. Examples include the prosecuting authorities (e.g. 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[5] to include the following factors in direction 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;

[5] Available from: https://www.judiciary.gov.uk/publications/criminal-practice-directions-2015/ [Accessed 05/10/15]

6. The completeness of the information which 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; and

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 haven't been taken into account, evidence may be excluded from 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[6] 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 that perform a similar task, even if the method or even tools are likely to be different.

4.4.2 Ultimately the end-user requirement is tailored to the implementing organisation, even different units in the same organisation may have subtly different requirements – e.g. methods for volume crime investigations may have different requirements than in counter terrorism.

4.4.3 When developing the end-user requirement, it is often useful to consider

[6] Accessed 24/11/15: https://www.gov.uk/government/collections/fsr-legal-guidance

if the expected output will be:

a. factual – absolutes (e.g. 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; or

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.

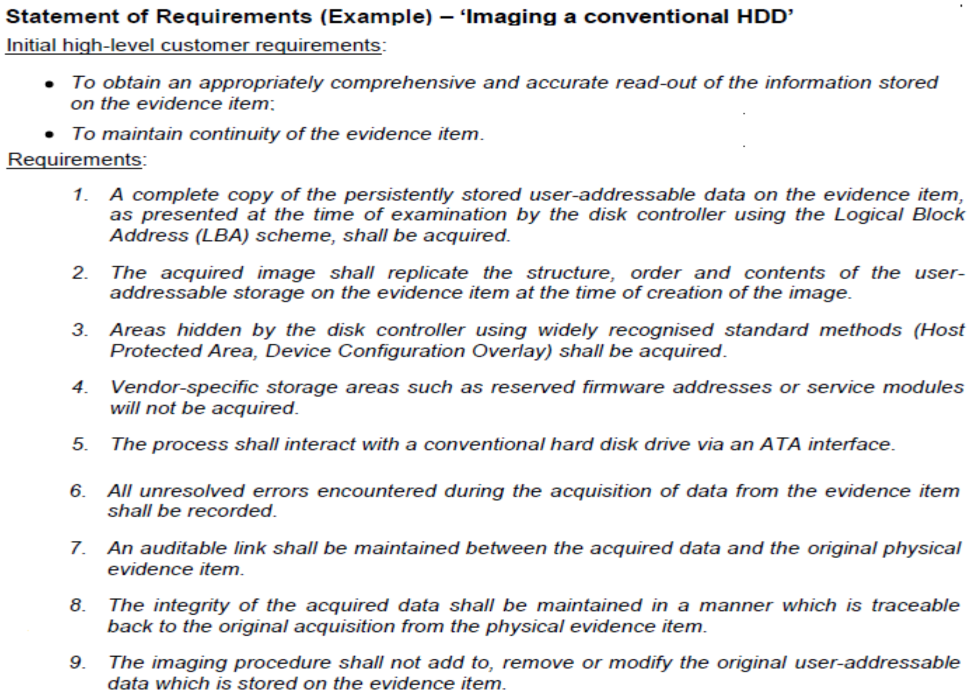
4.4.4 For example, if the method is to find JPEG[7] images by their file extensions then the requirement may be quite straightforward, as will the associated acceptance criteria and subsequent testing. If the user-requirement is to find <u>all</u> photographs (possibly including those partially overwritten) 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 going to be expected to do, and therefore validated to do. There may need to be iteration back with the user that 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 of the report needs to understand the limitations of the method, if the user understands this

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

then the acceptance criteria can be developed.

4.4.6 Text box 1 shows an example taken from a European Network of Forensic Science Institutes' document, showing the development of a high level requirement into a more technical requirement or even a start of a specification.



Statement of Requirements (Example) – 'Imaging a conventional HDD'

Initial high-level customer requirements:

- *To obtain an appropriately comprehensive and accurate read-out of the information stored on the evidence item;*
- *To maintain continuity of the evidence item.*

Requirements:

1. *A complete copy of the persistently stored user-addressable data on the evidence item, as presented at the time of examination by the disk controller using the Logical Block Address (LBA) scheme, shall be acquired.*
2. *The acquired image shall replicate the structure, order and contents of the user-addressable storage on the evidence item at the time of creation of the image.*
3. *Areas hidden by the disk controller using widely recognised standard methods (Host Protected Area, Device Configuration Overlay) shall be acquired.*
4. *Vendor-specific storage areas such as reserved firmware addresses or service modules will not be acquired.*
5. *The process shall interact with a conventional hard disk drive via an ATA interface.*
6. *All unresolved errors encountered during the acquisition of data from the evidence item shall be recorded.*
7. *An auditable link shall be maintained between the acquired data and the original physical evidence item.*
8. *The integrity of the acquired data shall be maintained in a manner which is traceable back to the original acquisition from the physical evidence item.*
9. *The imaging procedure shall not add to, remove or modify the original user-addressable data which is stored on the evidence item.*

From: ENFSI (2015) *Best Practice Manual for the Forensic Examination of Digital Technology,* ENFSI-BPM-FIT-01. Accessed 09/12/15 from: http://www.enfsi.eu/sites/default/files/documents/enfsi-bpm-fit-01_2.pdf

Text Box 1: Example of a Statement of Requirements for Imaging a Conventional Hard Disk Drive (HDD) being Developed into More Technical Requirements or Specification.

4.4.7 Like all statements of requirements, they are unique to an organisation or forensic unit. For example, an organisation might not require host projected areas or the device configuration overlay to be acquired. Accreditation requires a demonstration of technical competence which 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.

5 METHOD DEVELOPMENT

5.1.1 The methods used by organisations which perform digital forensics are almost always what the ISO17025 calls laboratory-developed methods. Laboratory-developed methods answer specific regularly requested needs by combining tools, techniques and expertise unique to the setup 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 setup/configuration of equipment is bespoke.

5.1.2 Prior to validation, the method needs to be precisely defined, the most appropriate way of doing this is to ensure 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.

5.1.3 If this is the first time the method is being 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.

5.1.4 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.

5.1.5 A thorough review of the requirements can ensure 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 wise at method development stage to design simple, yet effective, controls.

5.1.6 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 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 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.

6 RISK ASSESSMENT

6.1.1 An appropriate and realistic risk assessment is at the core of any validation study. The risks a method may pose dictate the focus of the validation exercise but must concentrate on realistic risks and not become an abstract ‘what if’ process.

6.1.2 Each risk assessment needs to be particular to the individual provider, 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 Criminal Justice System (CJS) often includes the:

a. the risk of wrongful conviction(s);

b. the risk of wrongful acquittal(s);

c. the risk of obstructing or delaying investigation(s).

6.1.3 It is important to know how a method or tool is to be used and importantly how they may provide misleading results in certain circumstances. The following summarises some of the sources of potential misleading results:[8]

a. Incompleteness.

b. Inaccuracy

   i. Existence: Do all artefacts reported as present actually exist?

   ii. Alteration: Does a forensic tool alter data in a way that changes its meaning, such as updating an existing date-time stamp (e.g. associated with a file or e-mail message) to the current date?

   iii. Association: For every set of items identified by a given tool, is each item truly a part of that set?

   iv. Corruption: Does the forensic tool detect and compensate for missing and corrupted data?

c. Misinterpretation.

6.1.4 From the above list the most common in many of the digital forensic applications is likely to be incompleteness, inability to recover or find all the data. Incompleteness is less likely to increase the risk of wrongful conviction, but it might prevent effective investigation and/or delay justice for victims. 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 which could create its own risk of some cases being turned away from having any digital examination due to the resource implications.

6.1.5 Should inaccuracy or misinterpretation occur the impact is more visible. Occasionally the courts to encounter such issues, but case law rarely comments on inability to find evidence as the case is less likely to have been put before them. Its impact should still be considered and the risk

[8] SWGDE (2015) *Establishing Confidence in Digital Forensic Results by Error Mitigation Analysis Version: 1.5.* Accessed 09/12/15: https://www.swgde.org/documents/Current%20Documents

proportionally mitigated against.

6.1.6 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.

6.1.7 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 the examination of mobile telephones[9] or encrypted systems that need to be powered on and live to allow access to the device. The risk of altering the data likely to be of interest needs to be assessed and managed.

6.1.8 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 really be that a method might not work, the risk is not being able to tell if it worked or not (e.g. a file search). The avoid, reduce or accept responses in traditional risk assessment processes apply. 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.

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

[9] The majority of mobile phone forensic software with write protect data at the logical, extent, level. However as the whole system is powered up memory management and where levying will still our at the binary level.

7 SCALE OF VALIDATION REQUIRED

7.1 Introduction

7.1.1 The scale of validation exercise will vary according to the complexity or novelty of a method, what data is available from previous studies, evaluations or validations, the risk assessment and finally what the end-user actually required the method to do.

7.1.2 Defining the specific purpose from the onset, focusing on starting with the most common functionality and requests should prevent the validation 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 provided actual competence to deliver valid results can be demonstrated.

7.1.3 Keeping in mind that the validation is about the method, the various types of validation studies tends 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 the data is available requires a critical review of validation records to ensure that the validation performed was fit for purpose and verification for the method to demonstrate that the unit is competent to perform the test/examination.

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

7.1.4 These three scenarios are complicated by the fact many methods may have been in use for a while but there is no or little available validation data. With a paucity of data 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 7.2 below with each individual organisation then evaluating the aspects of validation study performed by the collaborating third-parties as covered in section 7.3.

7.1.5 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 validity of the method used.

7.2 Novel Methods

7.2.1 If a method has been used in the digital forensics community for awhile but has no validation supporting it, or is entirely novel, then the validation required is often termed a developmental validation. This is opposed to an internal validation of a method adapted or adopted from elsewhere as it will require much more testing as there is no objective evidence of it being fit for purpose to draw upon. Methods adopted/adapted from elsewhere where pre-existing validation data is available is discussed in section 7.3.

7.2.2 The risk assessment (see section 6) of the method/user requirement is all about focussing 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.

7.2.3 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.

7.2.4 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 pass.

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

7.2.6 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 7.3 may well assist, once the software testing requirements are fulfilled.

7.2.7 The end-goal is that the implementing organisation, whether they developed the method or adopted/adapted the method, has similar objective evidence. The difference with a truly novel method is the amount of data generated by the implementing organisation is much greater, although the plus side is if this is a novel capability it may well be in great demand.

7.3 Adopted and Adapted Methods

7.3.1 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." (3.10)*

7.3.2 The above description (with emphasis added) is often referred collectively 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 you:

a. have something to review them against (i.e. an end-user requirement);

b. have 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.

7.3.3 Most fields in forensic science use some form of adopted methodology where some or all the validation data is available from elsewhere. As previously stated in paragraph 7.3.1, if another organisation has validated a method, complete re-validation may not be necessary but will require reviewing to see that it is fit for purpose based upon the available data. If the existing data does not cover the entire new requirement, or is deemed inadequate or unreliable, then before demonstrating competence to perform the method the, gaps in the objective evidence will need to be filled.

7.3.4 Before verification of performance, the provider 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.

7.3.5 A working understanding of experimental design is essential when validating new methods, but also important when assessing external validations.

7.3.6 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. However, objectively assessing published literature, software/hardware test results, and competency test results against known data is harder when differences in the user-requirements and methods are less likely to be visible.

7.3.7 The Regulator's more general guidance document on validation (FSR-G-201[10]) gives more detail on evaluating the reliability of externally derived objective evidence.

7.3.8 Detailed evaluations of tools used in a method such as produced in the United States of America by their National Institute of Standards and Technology[11] can be of great assistance; if a manufacturer or supplier of tools provides data this also can be objectively evaluated within the overall user-requirement of the method.

7.3.9 Once the method can be shown to be fit for purpose, there is a need to show that a provider's own competent staff can perform a method. This

[10] The Regulator's more general guidance document on validation (FSR-G-201) gives more detail on evaluating the reliability of external objective evidence, accessed 24/11/15: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/375285/FSR-G-201_Validation_guidance_November_2014.pdf#page=16

[11] Details of the their work is available from: http://www.cftt.nist.gov/ [accessed 24/11/15].

is where the validation has been conducted by the provider's own research or IT department and the method is being transferred to another location. A confirmation that the method is fit for purpose will be required along with documented evidence of the testing.

7.3.10 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 provider'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.

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

7.4 Minor Changes

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

7.4.2 The criteria for the risk assessment 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 which 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.

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

7.4.4 With the exception of methods which are almost entirely tool operation (e.g. a simple USB acquisition tool), most methods will have quality assurance stages, 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 had a range of tolerances methods where certain changes are anticipated may well have specified how this is assessed when small changes are required or even have this included in a change control or method modification protocol.

7.4.5 If a software tool is modified or changed, does this add new risks or are the existing validated quality assurance procedures already built into the method able to manage these risks?

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

7.4.7 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 will still apply, which will expect 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 and this may still mean the court can still adequately evaluate the findings. If the now new method is to become part of the routine activities of the provider, accreditation should always be sought.

7.4.8 Accreditation is about demonstrating competence, this can be taken to include the ability to correctly assess 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 it has a sufficient understanding of how changes may impact the results.

8 VALIDATION REQUIREMENTS AND ACCEPTANCE CRITERIA

8.1 Introduction

8.1.1 The validation requirements of a given method will depend on the tools employed, the risks and the output required. These should be defined at the outset of any validation testing, and should highlight:

a. any aspects of the method that directly impact the results or critical findings.

b. aspects of the method that that have lesser importance but may also be tested and assessed.

c. any issues expected (including any mitigation of these issues).

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

8.1.3 A validation or verification 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.

8.1.4 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 MAC or Linux then this would also need to be tested also.

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

8.2 Validation Strategy and Plan

8.2.1 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**,** which 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. Equipment, software or process under review.

 i. This should include all relevant details including the manufacturer, 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 as well.

 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.

8.3 Generation and Control of Test Data

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

8.3.2 If the method being tested is an adopted method, then the design of 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 designed to demonstrate it is fit for purpose as well demonstrating competence of the implementing organisation to perform the method.

8.3.3 Understanding the scale of the validation study you intend performing 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. It this is a verification of an existing adopted method validation study the same standard needs to be achieved.

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

8.3.5 Data or character types known to have caused problems with other methods. It should include wherever practicable, representative data types that the method is expected to be required to work on.

8.3.6 A sufficient quality and quantity of data to provide a rigorous assessment of the process.

8.3.7 This is known as stress testing. 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.

8.3.8 Data created for and/or generated during the validation should be stored for later audit, if required.

8.4 Undertaking Validation

(The Codes, 20.4–20.11, ISO/IEC17025:2005, 5.4.3–5.4.6)

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

8.4.2 As with most activities in forensic science, contemporaneous notes should 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. the expected outcome;

f. what the results were; and

g. any other appropriate information (e.g. the raw results or a link to them and where the test was performed, if this may affect findings).

8.5 Evaluation

8.5.1 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 as to whether the method has passed or failed each of the tests and is fit for purpose.

8.5.2 Testing should not normally be limited to a single attempt as there should be a consideration of uncertainty of measurement which usually is achieved by repeating tests, which can include:

a. duplicate equipment, calibrated in the same manner, run on the same data/in the same environment at the same time;

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 (perform search on large data set followed by search on smaller data set);

d. where the method to be portable (e.g. to be used at scenes) validation should include a robustness test to evaluate operation under different circumstances (e.g. temperature, humidity) without the occurrence of unexpected differences in the obtained result(s).

8.5.3 Any deviation from the plan, along with the reason for this, should be noted. 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.

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

a. A re-assessment 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;[12]

c. An assessment to consider if repeating the validation study or a new validation study is required.

[12] Changes to the method itself may have unintended consequences, whereas as an additional manual quality check may be assessed as acceptable.

9 CONCLUDING VALIDATION

(The Codes, 20.12–20.17)

9.1 Validation Report

9.1.1 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. define the required on-going quality regimen (e.g. quality assurance tests); and

iii. Effect of new approach/technique/equipment on existing methods: whether existing methods become obsolete and should be superseded or whether the method should be used as an alternative or in parallel.

9.2 Statement or Certificate of Validation Completion

9.2.1 The Codes require a statement or certificate of validation completion to 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 as the assessor should be suitably independent from those undertaking the validation study it could record that the method is not recommended for use.

9.2.2 Refer to the Codes for further details.

9.3 Implementation

9.3.1 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:

i. inclusion of the method in quality systems;

ii. on-going quality assurance should be defined.

c. Inclusion in existing systems (e.g. equipment logs, competency records, quality system).

10 POST-VALIDATION ACTIVITIES

(The Codes, 20.18., ISO/IEC17025:2005, 5.4.7)

10.1 Maintenance of Documentation

10.1.1 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 it. There may also be links to other requirements that are not directly concerned with validation, e.g. equipment logs detailing changes in use. The documentation should be updated as new major versions of software/equipment are tested and implemented.

10.2 Quality Assurance

10.2.1 The ongoing testing is recommended to ensure that equipment is being used correctly and the results should be recorded in the training and/or equipment documentation.

10.3 Acceptance Testing of New Equipment

10.3.1 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.

10.4 Review of Updates to Equipment or Software

10.4.1 It is in the nature of digital forensics for updates of software or equipment to be frequent however the overall method and its quality controls and output verification may be relatively stable. The method may be have been demonstrated to be robust to a range of changes particularly if the method has manual quality checks built into the method, however it is normal that the impact the change would have on the output of the method and the operation of the quality controls is carried out.

a. An acceptance test (or quality assurance test) is required to assess if the update affects the functionality or efficacy of the quality controls and output verification in the overall method, if this risk is identified then partial or full validation may be required.

b. Partial validation of the new functionality may be required if there is additional capability but the core capability remains unaltered (in addition, an acceptance test may still be required for the unaltered aspects as a safety check).

c. Full validation may be required if there have been changes across the equipment/software which result in a significant change to the method or output and operation.

11 ASSESSING UNCERTAINTY IN DIGITAL FORENSIC SCIENCE

11.1 Introduction

11.1.1 Forensic science is science applied in the service of the courts, the court and investigators for that matter, need to understand how accurate or complete a result or finding is.

11.1.2 For instance a timestamp is precise (e.g. 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 error and uncertainty might have on any inferences made from a timestamp. The requirement is to ensure that if uncertainty remains that the form of reporting correctly conveys this underlying uncertainty to ensure that the user of the information is not misled.

11.1.3 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 are assessed and reported with the results (see ISO17025 section 5.4.6.2).

11.1.4 In a search by file extensions for images, a factual report may stated that precisely x number of files were found, uncertainty may remain about how many images that were actually present on the media searched. This caveat might be entirely acceptable and understood for one application, in 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% in anything other than a dataset designed for evaluating a method should not be agreed to, likewise if there is always a possibility that some files might remain, an appropriate the caveat is often all that is required.

11.1.5 The uncertainty may be dealt with in the risk assessment of the method, it is covered separately here as it is a ISO17025 requirement and those conducting validations need to be aware of it. Assessing uncertainty is best addressed in the validation. Uncertainty may be presented in terms of false positive or negative (see section 6.1.2 on risk assessment) or in terms of accuracy and precision.

11.2 Accuracy

11.2.1 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.

11.2.2 For example, in an assessment of a search method in computing, this could be equated to whether all matching data are returned in a search as well as any matching data are not returned in a result.

11.3 Precision

11.3.1 Precision is synonymous with reproducibility or repeatability. An incorrectly calibrated device may be capable of giving reproducibly precise readings even though the data generated are not accurate. Precision is a measure of the uncertainty of the result, the type or range of results provided that are not *exactly* the true answer. In an assessment of a search method in computing, this could be equated to whether data returned varied each time a search was performed.

12 COMPETENCY

12.1 Introduction

12.1.1 Assessment of a method involves both the validity of the technique and the competency of the practitioner (both initial and on-going). As such, the ‘human factor’ needs to be accommodated into any method validation as the practitioner is part of the method.

12.2 Technical Skills

12.2.1 If a method is to be deployed without any interpretation (i.e. is a set of reproducible steps, none of which require a wider competence) then competence assurance can be limited to an assessment of whether a method is correctly applied by a practitioner.

12.3 Technical Interpretation

12.3.1 If a method is to be deployed where the result is not obvious to a layperson, technical interpretation will be required. The competence of the individual must be assessed to:

a. select the method;

b. apply the method; and

c. correctly interpret the output of the method.

12.4 Evaluative Opinion

12.4.1 Competence in the use of technical methods does not in itself provide any assurance that the output can be correctly interpreted when applied to a wider scenario or question.

12.4.2 In particular, opinion evidence (when a method is used to shed light on whether the evidence is expected given a specific activity) is prone to a range of additional concerns in addition to those concerning the validity of the method used. Competence in forensic interpretation (evaluative evidence) must be explicitly assessed if a practitioner is to produce opinion evidence. This would be in addition to validation exercises for a technical method and may require proficiency style exercises.

13 CONSEQUENCES OF FAILURE TO VALIDATE

13.1 Introduction

13.1.1 The examples provided are focused on specific areas of digital evidence, but the principles provided apply to all areas.

13.2 Sole Reliance on Case-By-Case Quality Assurance Procedures

13.2.1 It may be tempting to suggest that quality procedures implemented during the provision of casework (such as dual-tool verification and peer review) are adequate to demonstrate that the methods used are legitimate.

a. Dual-tool verification is a process that checks that one tool is producing the same results as another from the same exhibit on a case-by-case basis. However, both tools may share some of the same source code or libraries and could therefore produce the same erroneous results (i.e. they may be essentially the same tool with a different user interface). Unless the tools can be demonstrated to be truly independent there is no assurance that any correlation between outputs means that the results are legitimate. Validation of one or both tools should be undertaken to show this.

b. Peer review is an important tool for checking analyst competence, consistency of usage of methods, and error trapping on a case-by-case basis. However, peer review cannot assess whether the method used is producing reliable, repeatable results. The only assurance given for the methods used is that obvious errors or omissions from a method may be detected in the check.

13.2.2 Quality assurance should be built into a method that is being validated, and therefore the methods efficacy at controlling risk is tested in the validation study.

13.3 Validating Too Narrowly – i.e. Tool Rather than the Method

13.3.1 It is a method that produces the results, a tool is only part of a method. For example, a write blocker is a device that allows a storage device from an exhibit to be connected to a forensic examiner's computer, whilst preserving evidential integrity during preview or forensic imaging. It is important to verify that the write blocker is not malfunctioning, e.g. allowing data to be written back to the storage device or corrupting data as they are read through it. However, if this is the only part of the forensic imaging method that is checked or validated, it cannot be known whether consistent and full results are produced on each occasion. It is therefore important to validate the entire forensic imaging method, from the continuity and handling of the original exhibit through to the production of a verified set of forensic images for analysis, and including all intermediate steps.

13.4 Validating Only According to a Laboratory's Audit Schedule

13.4.1 Due to the reactive nature of casework it is often difficult to find time to review validation requirements. If a laboratory's requirements are not reviewed on a regular basis and only approached when there are impending deadlines to meet (e.g. the visit of an auditor) this could impact on the provision of up-to-date, fully validated services that a laboratory can offer.

14 REVIEW

14.1.1 When published, this document will be subject to review at regular intervals.

14.1.2 This version is a consultation draft so any comments please send them to FSRConsultation4@homeoffice.gsi.gov.uk as instructed on the front cover.

15 BIBLIOGRAPHY

Standards and related documents

BS EN ISO/IEC 17025:2005, *General requirements for the competence of testing and calibration laboratories.*

FSR (2014) *Codes of Practice and Conduct for Forensic Science Providers and Practitioners in the Criminal Justice System*. Forensic Science Regulator: Birmingham. Accessed 1/12/15: https://www.gov.uk/government/collections/forensic-science-providers-codes-of-practice-and-conduct.

FSR (2014) *Guidance: Validation*. *FSR-G-201, Issue 1.* Forensic Science Regulator: Birmingham. Accessed 09/12/15: https://www.gov.uk/government/publications/forensic-science-providers-validation.

ILAC G19:08/2014: *Modules in a Forensic Science Process*. Accessed 1/12/15: http://ilac.org/news/ilac-g19082014-published/.

Other documents

Criminal Practice Directions (2015*).* Accessed 07/12/15 : https://www.judiciary.gov.uk/publications/criminal-practice-directions-2015/.

Criminal Procedure Rules (2015). Published by the Ministry of Justice on behalf of the Criminal Procedure Rule Committee. Accessed 07/12/15: http://www.legislation.gov.uk/uksi/2015/1490/contents/made.

ENFSI (2015) *Best Practice Manual for the Forensic Examination of Digital Technology,* ENFSI-BPM-FIT-01. Accessed 09/12/15: http://www.enfsi.eu/sites/default/files/documents/enfsi-bpm-fit-01_2.pdf.

FSR (2015) Legal Obligations: Issue 3. Forensic Science Regulator: Birmingham Accessed 09/12/15: https://www.gov.uk/government/collections/fsr-legal-guidance.

SWGDE (2015) *Establishing Confidence in Digital Forensic Results by Error Mitigation Analysis Version: 1.5.* Accessed 09/12/15: https://www.swgde.org/documents/Current%20Documents

16 GLOSSARY

Accreditation

Third-party attestation related to a conformity assessment body conveying formal demonstration of the forensic science provider’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*.

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 or 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.

Customer

Whether internal or external, it is the organisation or the person who receives a product or service (e.g. the consumer, **end-user**, 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.

Evidence

Anything that may prove or disprove an assumption to be true, e.g. 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.

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 for solving a particular problem).

Organisation

A group of people and facilities with an arrangement of responsibilities, authorities and relationships (e.g. 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 service (e.g. scenes of crime, fingerprint bureau).

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.

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 (2015) there appears 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 and 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.

Validation

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

Verification

The context that it is used in 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."